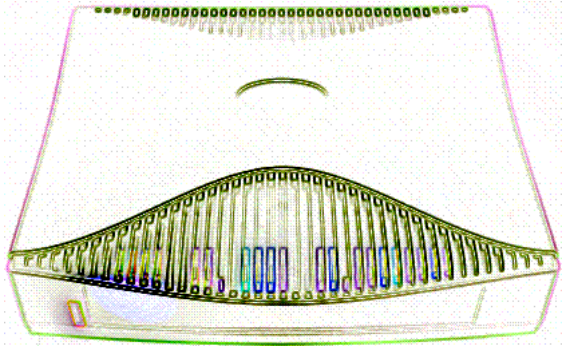
NETOPIA™ R310 ISDN ROUTER

User's Reference Guide



netopia®

Copyright

Netopia, Inc.
2470 Mariner Square Loop
Alameda, CA 94501-1010
U.S.A.

Part Number

For additional copies of this electronic manual, order Netopia part number 6161079-PF-02

Printed copies

For printed copies of this manual, order Netopia part number TER310/Doc
(P/N 6161079-00-02)

Contents

Welcome to the Netopia R310 *User's Reference Guide*. This guide is designed to be your single source for information about your Netopia R310 ISDN Router. It is intended to be viewed on-line, using the powerful features of the Adobe Acrobat Reader. The information display has been deliberately designed to present the maximum information in the minimum space on your screen. You can keep this document open while you perform any of the procedures described, and find useful information about the procedure you are performing.

This Table of Contents page you are viewing consists of hypertext links to the chapters and headings listed. If you are viewing this on-line, just click any link below to go to that heading.

Configuration options for your Netopia R310 ISDN Router

The Netopia R310 ISDN Router can be used in different ways depending on your needs. In general, you will probably want to use it in one or more of the following ways: (Click on one of these links)

- "1. Small Office connection to the Internet" with several computers in your office sharing a single IP address (Network Address Translation enabled)
- "2. Small Office connection to the Internet" with a block of IP addresses (Network Address Translation disabled),
- "3. Direct Connection to a Corporate Office (Telecommuter)"
- "4. Configured to accept incoming dial-up connections"

This section is intended to give you a path to the appropriate installation and configuration instructions based on your intended use for the Netopia R310 ISDN Router.

1. Small Office connection to the Internet

For Small Office connections to the Internet, using a single dynamic IP address with Network Address Translation (NAT) enabled, you should use the following configuration option:

- the SmartStart™ Wizard, included on your Netopia R310 CD.
  This is the fastest and simplest way to get you up and running with the minimum difficulty.

  For instructions on this option, see “Setting up your Router with the SmartStart Wizard” on page 3-3.

netopia®

2. Small Office connection to the Internet

For Small Office connections to the Internet, using a block of IP addresses (Network Address Translation disabled), you use both of the following configuration tools:

- the SmartStart™ Wizard, included on your Netopia R310 CD.
  This is the fastest and simplest way to get you up and running with the minimum difficulty.

  For instructions on this option, see “Setting up your Router with the SmartStart Wizard” on page 3-3.

- manual configuration using console-based management. This option allows maximum flexibility for experienced users and administrators.

  For instructions on this option, see “Console-based Management” on page 5-1.

3. Direct Connection to a Corporate Office (Telecommuter)

For direct connections to a Corporate Office, you can use either one of two configuration options:

- the SmartStart™ Wizard, included on your Netopia R310 CD.

  For instructions on this option, see “Setting up your Router with the SmartStart Wizard” on page 3-3.

- manual configuration using console-based management. This option allows maximum flexibility for experienced users and administrators.

  For instructions on this option, see “Console-based Management” on page 5-1.

4. Configured to accept incoming dial-up connections

To configure the Netopia R310 to accept incoming dial-up connections, you should use the following configuration option:

- use the SmartStart™ Wizard, to configure your outbound connection to an ISP.

  For instructions on this option, see “Setting up your Router with the SmartStart Wizard” on page 3-3.

- manual configuration using console-based management. You will go to WAN configuration and add one or more dial-in Connection Profiles.

  For instructions on this option, see “Creating a new Connection Profile” on page 7-1.


netopia

Part I: Getting Started

Chapter 1

Introduction

Overview

The Netopia R310 ISDN Router is a full-featured, stand-alone, multiprotocol router for connecting diverse local area networks (LANs) to the Internet and other remote networks. The Netopia R310 ISDN Router uses a high performance telecommunications line to provide your whole network with a high-speed connection to the outside world.

This section covers the following topics:

Features and capabilities

The Netopia R310 ISDN Router provides the following features:

- Support for IP routing for Internet and Intranet connectivity
- IP address serving (over Ethernet or a WAN link) which allows local or remote network nodes to automatically acquire an IP address dynamically from a designated pool of available addresses
- WAN connection over an ISDN phone line, switched, or leased,
- Support for Ethernet LANs with multiple Ethernet IP subnets
- Advanced ISDN cost control through scheduled connections and call accounting of both aggregate and per-profile statistics
- Console-based Telnet client
- UNIX syslog client
- Status lights (LEDs) for easy monitoring and troubleshooting
- SmartStart™ Wizard software for easy configuration over an Ethernet network connection. The SmartStart Wizard may include an optional automatic registration with one of several major ISPs, making the process as simple as completing a registration form. Using the alternate manual setting to configure the router for an ISP that's not listed, the software allows you to configure your internal connection by entering just five fields: username, password, dialup number, DNS, and IP gateway.
- Support for Console-based management
- SmartIP™ for simple and economical to connect a workgroup of users to the Internet or a remote IP network by using Network Address Translation and a single IP address.
- Wall-mountable, Bookshelf (Side-stackable), or Desktop-stackable design for efficient space usage

How to use this guide

In addition to the simple documentation contained in the accompanying *Getting Started Guide*, this guide is designed to be your single source for information about your Netopia R310 ISDN Router. It is intended to be viewed on-line, using the powerful features of the Adobe Acrobat Reader. The information display has been deliberately designed to present the maximum information in the minimum space on your screen. You can keep this document open while you perform any of the procedures described, and find useful information about the procedure you are performing.

You can also print out all of the manual, or individual sections, if you prefer to work from hard copy rather than on-line documentation. The pages are formatted to print on standard 8 1/2 by 11 inch paper. We recommend that you print on 3-hole punched paper, so that you can put the pages in a binder for future reference. For your convenience, a printed copy is available from Netopia. Order part number TER310/Doc.

This guide is organized into chapters describing the Netopia R310's advanced features. You may want to read each chapter's introductory section to familiarize yourself with the various features available.

Use the guide's table of contents and index to locate informational topics.

Chapter 2

Making the Physical Connections

This section tells you how to make the physical connections to your Netopia R310 ISDN Router. This section covers the following topics:

Find a location

When choosing a location for the Netopia Router, consider:

- Available space and ease of installation
- Physical layout of the building and how to best use the physical space available in relation to connecting your Netopia Router to the LAN
- Available wiring and jacks
- Distance from the point of installation to the next device (length of cable or wall wiring)
- Ease of access to the front of the unit for configuration and monitoring
- Ease of access to the back of the unit for checking and changing cables
- Cable length and network size limitations when expanding networks

For small networks, install the Netopia R310 near one of the LANs. For large networks, you can install the Netopia R310 in a wiring closet or a central network administration site.

What you need

Locate all items that you need for the installation.

Included in your router package are:

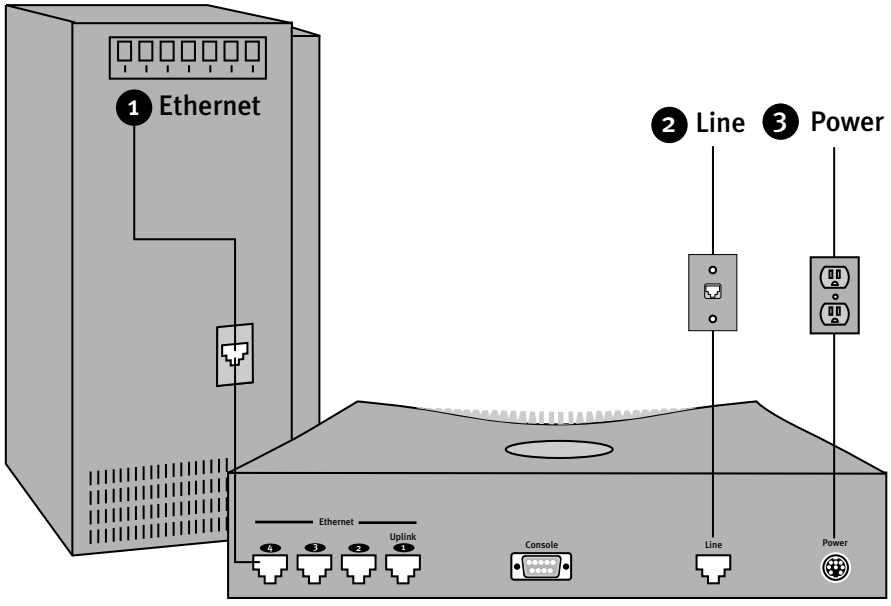
- The Netopia R310 ISDN Router
- A power adapter and cord
- An Ethernet cable (RJ-45) to connect one computer to the built-in 10BaseT hub
- An ISDN cable (RJ-45) to attach to your Telco or Line port
- A cross-over cable
- The Netopia CD containing the SmartStart Wizard, this documentation, an Internet browser, Adobe® Acrobat® Reader for Windows and Macintosh, ZTerm terminal emulator software and NCSA Telnet 2.6 for Macintosh

You will need:

- A Windows 95, 98, or NT-based PC or a Macintosh with Ethernet connectivity for configuring the Netopia R310. This may be built-in Ethernet or an add-on card, with TCP/IP installed.
- An ISDN telephone line.

Identify the connectors and attach the cables

Identify the connectors and switches on the back panel and attach the necessary Netopia Router cables.



1. Connect one of the RJ-45 cables to any of the Ethernet ports on the router.

   (If you are connecting the router to an existing Ethernet hub, use Ethernet port #1/Uplink on the router and an Ethernet crossover cable.)

2. Connect one end of one of the RJ-45 cables to the Line port, and the other end to your ISDN line wall jack.
3. Connect the Power Adapter to the Power port, and plug the other end into an electrical outlet.

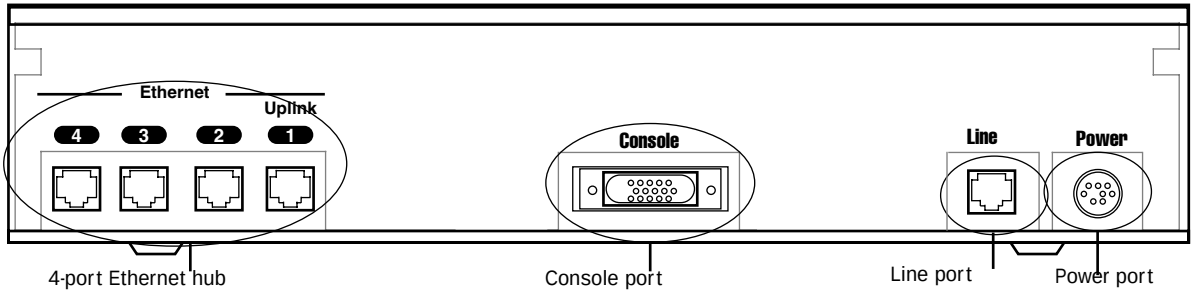
   You should now have: the power adapter plugged in; the Ethernet cable connected between the router and your computer; and the telephone cables connected between the router and the ISDN line wall jack.

4. Insert your Netopia CD and follow the instructions to install an Internet browser and the Adobe Acrobat Reader, if you don't already have them.

Netopia R310 ISDN Router Back Panel Ports

The figure below displays the back of the Netopia R310 ISDN Router.

Netopia R310 ISDN Router back panel



The following table describes all the Netopia R310 ISDN Router back panel ports.

Port	Description
Power port	A power adapter cable connection.
Line port	An RJ-45 jack for your WAN connection.
Console port	A DB-9 console port for a direct serial connection to the console screens. You can use this if you are an experienced user. See Chapter 5, “Console-based Management.”
4-port Ethernet hub	Four Ethernet jacks. You will use one of these to connect to the Netopia R310 for configuration. For a new installation with SmartStart, use the Ethernet connection. You can either connect your computer directly to any of the Ethernet ports on the router, or connect both your computer and the router to an existing Ethernet hub on your LAN. Alternatively, you can use the console connection with a terminal emulator application and a direct serial connection, or Telnet via Ethernet, to run console-based management. See Chapter 5, “Console-based Management.”

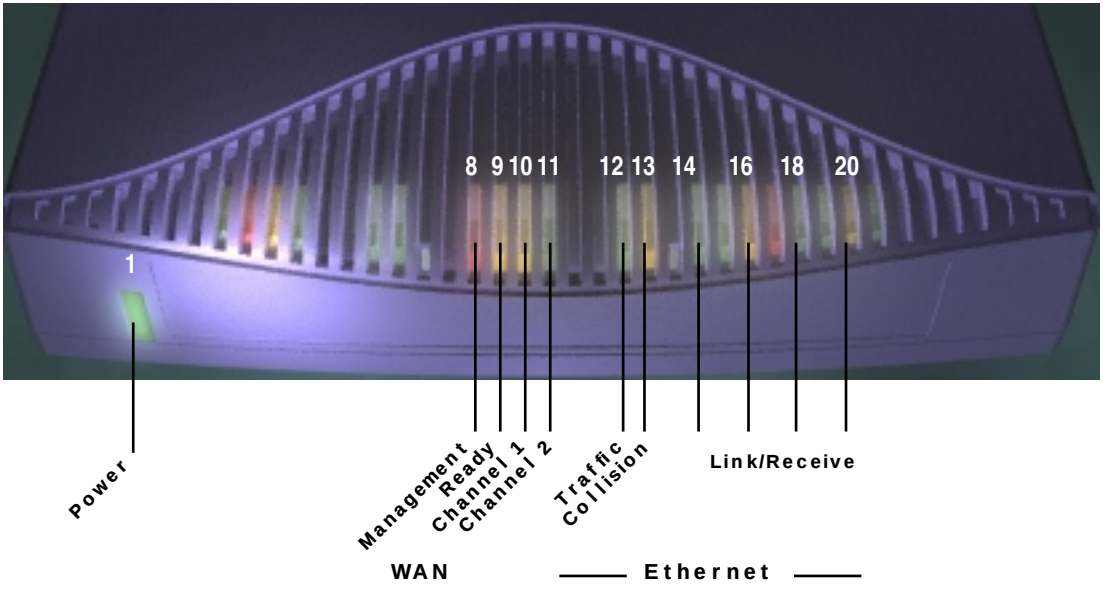
*** Note:** Users in the United Kingdom may need to obtain a special US-to-UK style modular connector adapter. Suitable adapters are available as follows:

Supplier	Phone No	Product Code
Black Box www.blackbox.co.uk	0118 9655100	MCU9413
Maplins Electronics www.maplin.co.uk	01702 554000	VD36

Netopia R310 ISDN Router Status Lights

The figure below represents the Netopia R310 status light (LED) panel.

Netopia R310 LED front panel



The following table summarizes the meaning of the various LED states and colors:

When this happens...	the LEDs...
Power is on	1 is **green**.
Data is transmitted or received over the ISDN D channel	8 flashes **orange**.
The WAN interface is operational	9 is **green**.
The WAN interface is inactive	9 is **off**.
The WAN interface detects a failure after line activation	9 flashes **red**.
Calls are setting up	10 and 11 flash **green**.
Data calls connect	10 and 11 are **green**.
The line is carrying data traffic	10 and 11 pulse **orange**.
The respective Ethernet port is connected to the LAN	14, 16, 18, and 20 are **green**.
There is activity on the respective Ethernet ports	14, 16, 18, and 20 flash **green**.
Note: 2 through 7, 15, 17, 19, and 21 are unused.	

Chapter 3

Setting up your Router with the SmartStart Wizard

Once you've connected your router to your computer and your telecommunications line and installed a web browser, you're ready to run the Netopia SmartStart™ Wizard. The SmartStart Wizard will help you set up the router and share the connection. The SmartStart Wizard walks you through a series of questions and based on your responses automatically configures the router for connecting your LAN to the Internet or to your remote corporate network.

The SmartStart Wizard will:

- automatically check your Windows 95, 98, or NT PC's TCP/IP configuration to be sure you can accept a dynamically assigned IP address, and change it for you if it is not set for dynamic addressing
- check the physical connection from your computer to your router without your having to enter an IP address
- assign an IP address to your router
- allow you to register with a new ISP if you don't already have one
- allow you to enter your dial-up telephone numbers and other information, dial up and test your connection to your chosen ISP or other remote site

This chapter covers the following topics:

Before running SmartStart

Be sure you have connected the cables and power source as described in "Identify the connectors and attach the cables" on page 2-2.

Before you launch the SmartStart application, make sure your computer meets the following requirements:

	PC	Macintosh
System software	Windows 95, 98, or NT operating system	MacOS 7.5 or later
Connectivity software	TCP/IP must be installed and properly configured. See "Configuring TCP/IP on Windows 95, 98, or NT computers" on page 3-9	MacTCP or Open Transport TCP/IP must be installed and properly configured. See "Configuring TCP/IP on Macintosh computers" on page 3-12.
Connectivity hardware	Ethernet card (10Base-T)	Either a built-in or third-party Ethernet card (10Base-T)
Browser software	Netscape Communicator™ or Microsoft Internet Explorer, included on the Netopia CD. Required for web-based registration and web-based monitoring.	

Notes:

- The computer running SmartStart must be on the same Ethernet cable segment as the Netopia R310. Repeaters, such as 10Base-T hubs between your computer and the Netopia R310, are acceptable, but devices such as switches or other routers are not.
- SmartStart for the PC will set your TCP/IP control panel to "Obtain an IP address automatically" if it is not already set this way. This will cause your computer to reboot. If you have a specified IP address configured in the computer, you should make a note of it before running SmartStart, in case you do not want to use the dynamic addressing features built in to the Netopia Router and need to restore the fixed IP address.

Setting up your Router with the SmartStart Wizard

The SmartStart Wizard is tailored for your platform, but it works the same way on either a PC or a Macintosh. Insert the Netopia CD, and in the desktop navigation screen that appears, launch the SmartStart Wizard application.

SmartStart Wizard configuration screens

The screens described in this section are the default screens shipped on the Netopia CD. They derive from two initialization (.ini) files included in the same directory as the SmartStart application file. Your reseller or your ISP may have supplied you with customized versions of these files.

- If you have received a CD or diskette that has been customized by your reseller or ISP, you can run the SmartStart Wizard directly from the CD or diskette and follow the instructions your reseller or ISP provides. This makes your Netopia R310 configuration even easier.
- If you have received only the .ini files from your reseller or ISP, perform the following:
  - Copy the entire directory folder containing the SmartStart Wizard application from the Netopia CD to your hard disk.
  - Copy the customized .ini files to the same directory folder that contains the SmartStart Wizard application, allowing the copy process to overwrite the original .ini files.
  - Run the SmartStart Wizard from your hard disk. You can then follow the instructions your reseller or ISP provides.

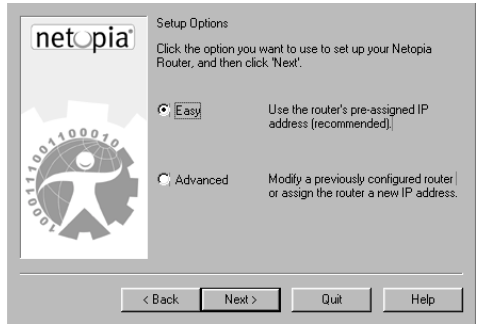
The SmartStart Wizard presents a series of screens to guide you through the preliminary configuration of a Netopia R310. It will then create a connection profile using the information you supply to it.

Welcome screen. The first screen welcomes you to the SmartStart Wizard configuration utility.

Click the Next button after you have responded to the interactive prompts in each screen.

The Help button will display useful information to assist you in responding to the interactive prompts.

Easy or Advanced options screen. You can choose either Easy or Advanced setup.



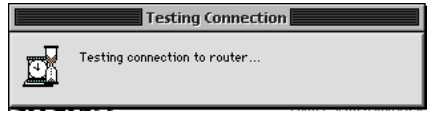
- If you choose Easy, SmartStart automatically uses the preconfigured IP addressing setup built into your router. This is the best choice if you are creating a new network or don't already have an IP addressing scheme on your new network.

  If you choose Easy, you will see a "Connection Test screen," like the one shown below while SmartStart checks the connection to your router.

- If you choose Advanced, skip to page 3-8 now. The SmartStart Wizard displays the "Router IP Address screen" on page 3-8, in which you can choose ways to modify your router's IP address.

Easy option

Connection Test screen. SmartStart tests the connection to the router. While it is testing the connection, a progress indicator screen is displayed and the router's Ethernet LEDs flash.



When the test succeeds, SmartStart indicates success and presents one of the screens on the next page.

If the test fails, the wizard displays an error screen. If the test fails, check the following:

- Check your cable connections. Be sure you have connected the router and the computer properly, using the correct cables. See "Identify the connectors and attach the cables" on page 2-2.
- Make sure the router is turned on and that there is an Ethernet connection between your computer and the router.
- Check the TCP/IP control panel settings to be sure that automatic IP Addressing (Windows) or DHCP (Macintosh) is selected. If you are using a Windows PC, SmartStart will automatically detect a static IP address and offer to configure the computer for automatic addressing. On a Macintosh computer, you must manually set the TCP/IP Control Panel to DHCP. See "Configuring TCP/IP on Macintosh computers" on page 3-12. If you currently use a static IP address outside the 192.168.1.x network, and want to continue using it, use the Advanced option to assign the router an IP address in your target IP range. See "Advanced option" on page 3-8.
- If all of the above steps fail to resolve the problem, reset the router to its factory default settings and rerun SmartStart. See "Factory defaults" on page 13-7 for more information.

When the test is successful, SmartStart presents you with a different screen, depending on the type of router you are configuring.

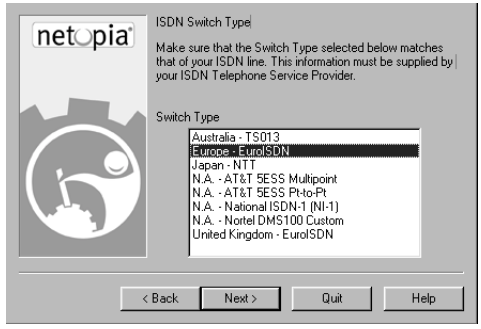
- You may see the "ISDN Switch Type screen," shown below, displaying the possible switch types available for your region. However, this screen may not appear if there is only one switch type in use in your region, if you are using a customized version of SmartStart, or if the ISDN Wizard has automatically detected your switch type.

ISDN Switch Type screen. The ISDN Switch Type screen appears.

Select one of the supported ISDN switch types for your ISDN line. Your telephone company should have provided this information when your ISDN line was installed.

When you have done this, click Next.

Note: The switch types listed are different for different regions. If your region has only one switch type, this screen may not appear.

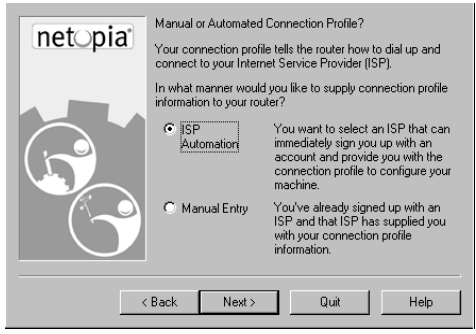


- Next you will see the "Manual or Automated Connection Profile screen," shown below.

Manual or Automated Connection Profile screen. The SmartStart Wizard asks you to select a method of creating a connection profile. The connection profile tells your router how to communicate with your ISP or other remote site, such as your corporate office. You can select either ISP Automation or Manual Entry.

Options are explained below.

Make your selection and click Next.



If you select ISP Automation, SmartStart offers you the option of choosing one of several Netopia ISP partners that support the Netopia R310. You then see the "Internet Service Provider Selection screen" on page 3-6.

If you select Manual Entry, you must be prepared with the following information. You must enter:

- Your dial-up number, sometimes referred to as an ISP POP number
- Your Login name and Password. (These are case-sensitive.)
- Any PBX or Centrex phone system dialing prefix (such as "9" for an outside line)
- Your PPP authentication method. Options are: PAP (Password Authentication Protocol), CHAP (Challenge Handshake Authentication Protocol), or None. Most ISPs use PAP; this is the default.
- Your Domain Name Server (DNS); this entry must be an IP address in dotted decimal format. (for example, 192.168.4.10, not "joe.isp.com")

- Optionally, an alternate DNS if your ISP provided one

If you select Manual Entry, the "Connection Profile screen," shown below appears.

Internet Service Provider Selection screen. Select an ISP from the list of Netopia ISP partners who have provided information for automatic setup. Choose Generic ISP if your ISP is not included on the list. If you don't already have an account with the selected ISP, call and order service using the listed customer service telephone number.

When you have done this, click Next.

- Most ISPs will provide you with information for you to enter in the "Connection Profile screen" on page 3-6 (shown below) over the phone using the toll-free phone number shown in the scrolling list. Generally, they will provide you with:
  - Your dial-up number, sometimes referred to as an ISP POP number
  - Your Login name and Password. (These are case-sensitive.)

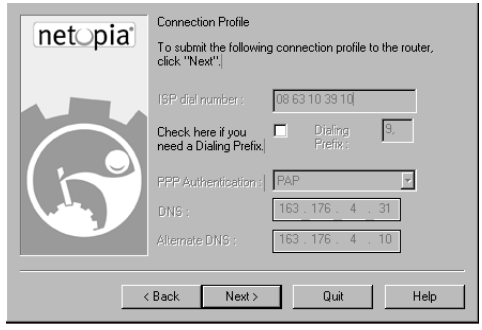
  Note: Your ISP may provide you with additional values such as "Remote IP Gateway" or "Subnet Mask." These entries are not required for the SmartStart Wizard to configure your router.

  If you have a PBX or Centrex phone system, you may need a dialing prefix (such as "9" for an outside line). You will enter that information in the "Connection Profile screen," shown below.

Connection Profile screen. Enter your ISP-supplied configuration information mentioned above. All fields must be filled in except the Alternate DNS field if your ISP does not provide one. If your ISP appeared in the "Internet Service Provider Selection screen" on page 3-6 your ISP will already have provided much of the information required for the connection, and these fields will appear grayed-out.

When you have done this, click Next.

The "Name and Password screen" on page 3-7 appears; this is where you enter the username and password for your connection to your ISP.



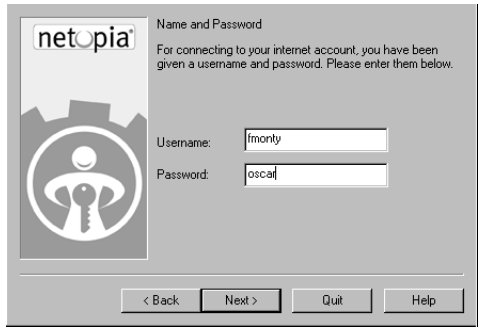
Name and Password screen. Enter the username and password that identifies you to your ISP.

Note: Some automated profiles already specify name and password for you. in this case, the screen is filled out for you and automatically skipped.

When you have done this, click Next.

The SmartStart Wizard then posts your connection profile information to your router.

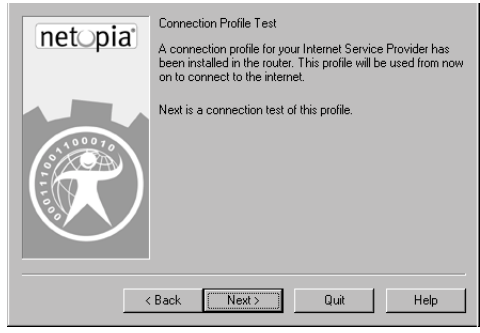
Now the "Connection Profile Test screen," (shown below) appears. It allows you to test your connection to your ISP using the connection profile you have just created.



Connection Profile Test screen. SmartStart tests your connection profile by attempting to connect to your ISP.

To test the connection profile with your ISP, click Next.

While the test is running, SmartStart reports its progress in a brief succession of dialog boxes as described below.



Available Line Test Progress screen. SmartStart tests to see if the router can place calls on your telephone line. While it is testing the connection, a dialog box is displayed and the LEDs flash.

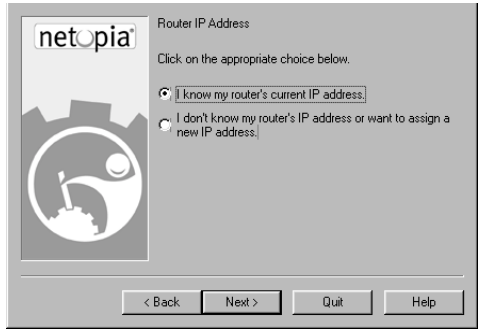
Connection Test Progress screen. SmartStart displays a dialog box showing you that your connection profile is being tested. If this test fails, check the physical connections between the computer, the router, and the wall jack or jacks. Check for errors in any manual entries you made during the configuration process.

Final screen. When the connection tests successfully, SmartStart displays a screen telling you that your configuration is now complete.

In most cases, this SmartStart configuration is all that you need to get your router up and running and connected to the Internet. However, you may want to take advantage of additional features or special configuration options available through the console-based configuration interface. For detailed instructions, see "Console-based Management" on page 5-1.

Advanced option

Router IP Address screen. If you selected the Advanced option in the "Easy or Advanced options screen" on page 3-4, SmartStart asks you to choose between entering the router's current IP address and assigning an IP address to the router.

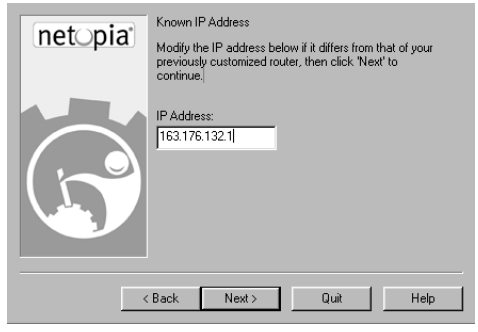


If the router has already been assigned an IP address, select the first radio button. If you do this, the "Known IP Address screen," appears (shown below.)

If you want to reconfigure the router with a new IP address and subnet mask, select the second radio button. If you do this, the "New IP Address screen" on page 3-9 appears.

When you have done this, click Next.

Known IP Address screen. SmartStart displays a recommended address for the router based on the IP address of the computer.



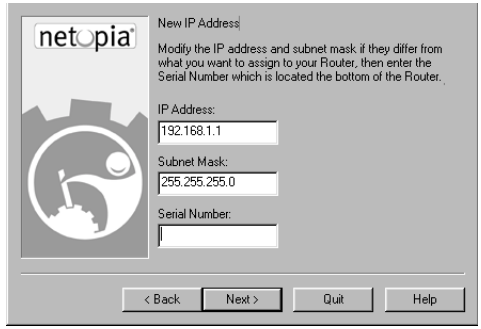
If you know the router has an IP address different from the default value, enter it now. Otherwise, accept the recommended address.

When you have done this, click Next.

SmartStart tests the connection to your router.

SmartStart then returns you to the "Connection Profile screen" on page 3-6.

New IP Address screen. If you want to change the router's IP address, you enter the new IP address, the subnet mask, and the router's serial number in this screen. Remember, the serial number is on the bottom of the router.



Note: Forcing a new IP address may turn off the Netopia R310's IP address serving capabilities, if you assign an IP address and subnet mask outside the router's current IP address serving pool. The Netopia R310 does not allow an invalid address to be served. Use this option with caution.

When you have done this, click Next.

SmartStart forces the new IP address into the router, tests the connection, and then resets the router.

SmartStart then returns you to the "Connection Profile screen" on page 3-6.

Sharing the Connection

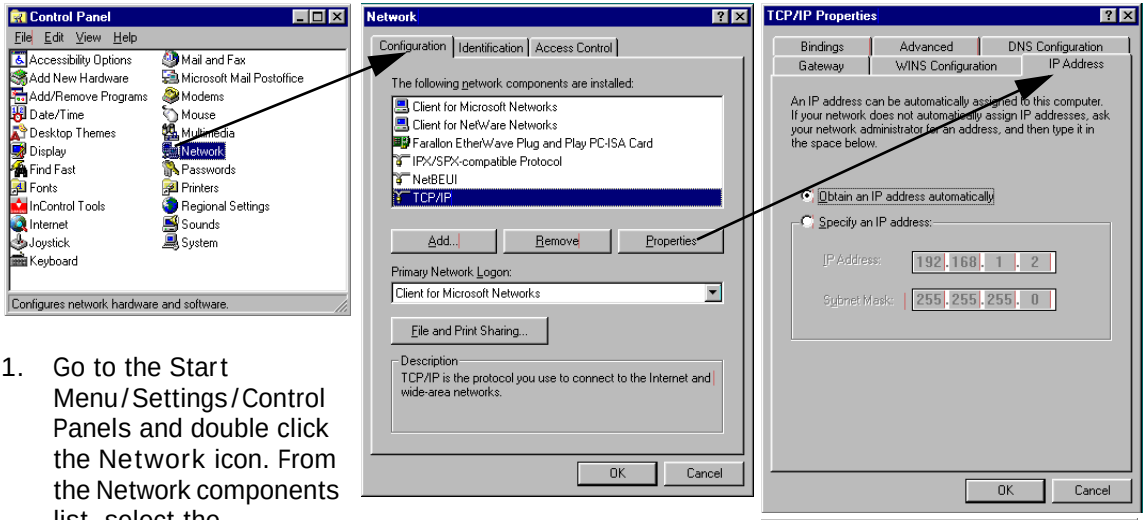
Configuring TCP/IP on Windows 95, 98, or NT computers

Configuring TCP/IP on a Windows computer requires the following:

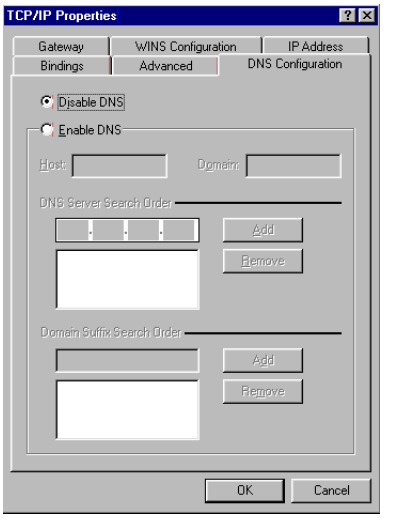
- An Ethernet card (also known as a network adapter)
- The TCP/IP protocol must be "bound" to the adapter or card

Dynamic configuration (recommended)

If you configure your Netopia R310 using SmartStart, you can accept the dynamic IP address assigned by your router. The Dynamic Host Configuration Protocol (DHCP) server, which enables dynamic addressing, is enabled by default in the router. If your PC is not set for dynamic addressing, SmartStart will offer to do this for you when you launch it. In that case, you will have to restart your PC and relaunch SmartStart. If you configure your PC for dynamic addressing in advance, SmartStart need only be launched once. To configure your PC for dynamic addressing do the following:



1. Go to the Start Menu/Settings/Control Panels and double click the Network icon. From the Network components list, select the Configuration tab.
2. Select TCP/IP-->Your Network Card. Then select Properties. In the TCP/IP Properties screen (shown below), select the IP Address tab. Click "Obtain an IP Address automatically."
3. Click on the DNS Configuration tab. Click Disable DNS. DNS will be assigned by the router with DHCP.
4. Click OK in this window, and the next window. When prompted, reboot the computer.

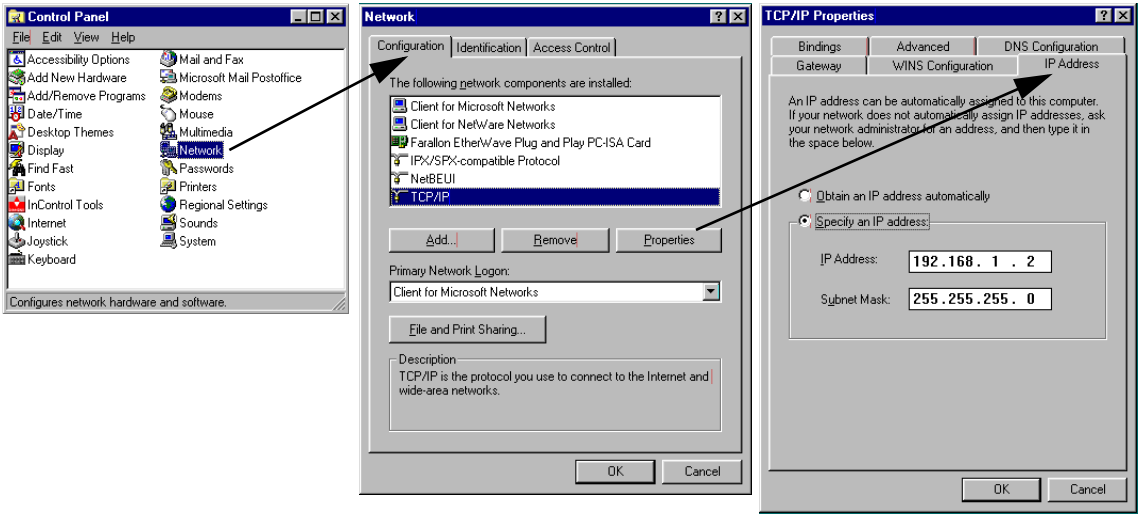


Note: You can also use these instructions to configure other computers on your network to accept IP addresses served by the Netopia R310.

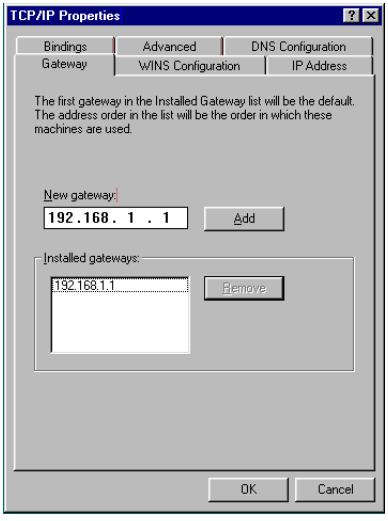
Static configuration (optional)

If you are manually configuring for a fixed or static IP address, perform the following:

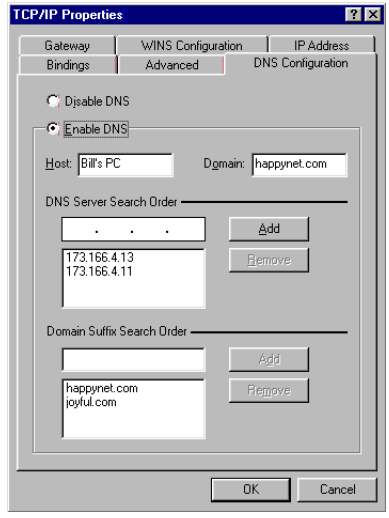
1. Go to Start Menu/Settings/Control Panels and double click the Network icon. From the Network components list, select the Configuration tab.
2. Select TCP/IP-->Your Network Card. Then select Properties. In the TCP/IP Properties screen (shown below), select the IP Address tab. Click “Specify an IP Address.”
   Enter the following:
   IP Address: 192.168.1.2
   Subnet Mask: 255.255.255.0
   This address is an example of one that can be used to configure the router with the Easy option in the SmartStart Wizard. Your ISP or network administrator may ask you to use a different IP address and subnet mask.



3. Click on the Gateway tab (shown below). Under "New gateway," enter 192.168.1.1. Click Add. This is the Netopia R310's pre-assigned IP address.



Click on the DNS Configuration tab. Click Enable DNS. Enter the following information:



Host: Type the name you want to give to this computer.

Domain: Type your domain name. If you don't have a domain name, type your ISP's domain name; for example, netopia.com.

DNS Server Search Order: Type the primary DNS IP address given to you by your ISP. Click Add. Repeat this process for the secondary DNS.

Domain Suffix Search Order: Enter the same domain name you entered above.

4. Click OK in this window, and the next window. When prompted, reboot the computer.

Note: You can also use these instructions to configure other computers on your network with manual or static IP addresses. Be sure each computer on your network has its own IP address.

Configuring TCP/IP on Macintosh computers

The following is a quick guide to configuring TCP/IP for MacOS computers. Configuring TCP/IP in a Macintosh computer requires the following:

- You must have either Open Transport or Classic Networking (MacTCP) installed.

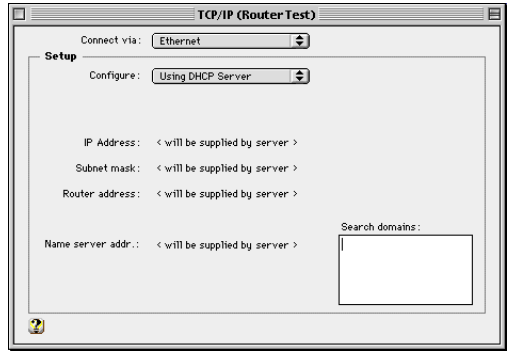
  Note: If you want to use the Dynamic Host Configuration Protocol (DHCP) server built into your Netopia R310 to assign IP addresses to your Macintoshes, you must be running Open Transport, standard in MacOS 8, and optional for MacOS 7.5 and above.

- You must have built-in Ethernet or a third-party Ethernet card and its associated drivers installed in your Macintosh.

Dynamic configuration (recommended)

If you configure your Netopia R310 using SmartStart, you can accept the dynamic IP address assigned by your router. The Dynamic Host Configuration Protocol (DHCP), which enables dynamic addressing, is enabled by default in the router. To configure your Macintosh computer for dynamic addressing do the following:

1. Go to the Apple menu. Select Control Panels and then TCP/IP.
2. With the TCP/IP window open, go to the Edit menu and select User Mode. Choose Basic and click OK.
3. In the TCP/IP window, select “Connect via: Ethernet” and “Configure: Using DHCP Server.”



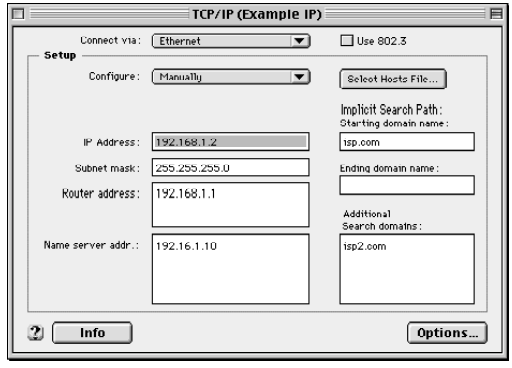
Note: You can also use these instructions to configure other computers on your network to accept IP addresses served by the Netopia R310.

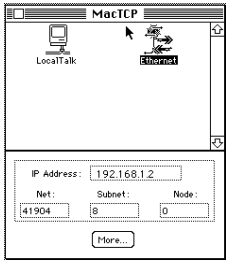
Static configuration (optional)

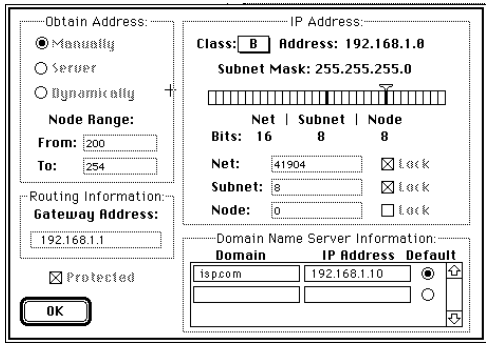
If you are manually configuring the computer on your Local Area Network for a fixed or static IP address, perform the following:

1. Go to the Apple menu. Select Control Panels and then TCP/IP or MacTCP.
2. With the TCP/IP window open, go to the Edit menu and select User Mode. Choose Advanced and click OK.

   Or, in the MacTCP window, select Ethernet and click the More button.







3. In the TCP/IP window or in the MacTCP/More window, select or type information into the fields as shown in the following table.

Option:	Select / Type:
Connect via:	Ethernet
Configure:	Manually
IP Address:	192.168.1.2
Subnet mask:	255.255.255.0, or for 12-user models, 255.255.255.240
Router address:	192.168.1.1
Name server address:	Enter the primary and secondary name server addresses given to you by your ISP
Implicit Search Path: Starting domain name:	Enter your domain name; if you do not have a domain name, enter the domain name of your ISP

4. Close the TCP/IP or MacTCP control panel and save the settings.
5. If you are using MacTCP, you must restart the computer. If you are using Open Transport, you do not need to restart.

   These are the only fields you need to modify in this screen.

Note: You can also use these instructions to configure other computers on your network with manual or static IP addresses. Be sure each computer on your network has its own IP address.

DNS Proxy and Caching Behavior

Please note, DNS Proxying is a standard Netopia router feature. This feature operates transparently with no configuration required.

If the Netopia R310's DNS is 0.0.0.0 the router serves itself as the DNS to DHCP client workstations that are configured to acquire their IP addresses dynamically. If the router obtains a valid DNS supplied by the ISP, it does one of two things:

- either it forwards all DNS requests it receives to its DNS and remaps them when the response is received, or
- it constructs a DNS response if it finds the mapping in its own DNS cache.

This ensures that DHCP clients of the Netopia R310 will be able to use DNS as soon as the NetopiaR310 is able to do so.

If the Netopia R310 is rebooted in a state wherein its DNS is non-zero, then the router will thereafter seed its DHCP clients with the router's DNS.

If for any reason you want to use the Netopia R310's DNS proxy feature all the time, then you manually configure your client workstations' IP stack so that your DNS is the Netopia R310.

Chapter 4

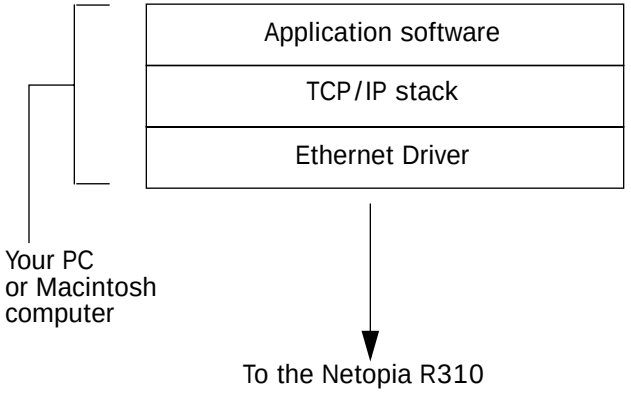
Connecting Your Local Area Network

This chapter describes how physically to connect the Netopia R310 ISDN Router to your local area network (LAN). Before you proceed, make sure the Netopia R310 is properly configured. You can customize the Router's configuration for your particular LAN requirements using Console-based Management (see "Console-based Management" on page 5-1).

This section covers the following topics:

Readying computers on your local network

PC and Macintosh computers must have certain components installed before they can communicate through the Netopia R310. The following illustration shows the minimal requirements for a typical PC or Macintosh computer.



Application software: This is the software you use to send e-mail, browse the World Wide Web, read newsgroups, etc. These applications may require some configuration. Examples include the Eudora e-mail client, and the web browsers Microsoft Internet Explorer and Netscape Navigator.

TCP/IP stack: This is the software that lets your PC or Macintosh communicate using Internet protocols. TCP/IP stacks must be configured with some of the same information you used to configure the Netopia R310. There are a number of TCP/IP stacks available for PC computers. Windows 95 includes a built-in TCP/IP stack. See "Configuring TCP/IP on Windows 95, 98, or NT computers" on page 3-9. Macintosh computers use either MacTCP or Open Transport. See "Configuring TCP/IP on Macintosh computers" on page 3-12.

Ethernet: Ethernet hardware and software drivers enable your PC or Macintosh computer to communicate on the LAN.

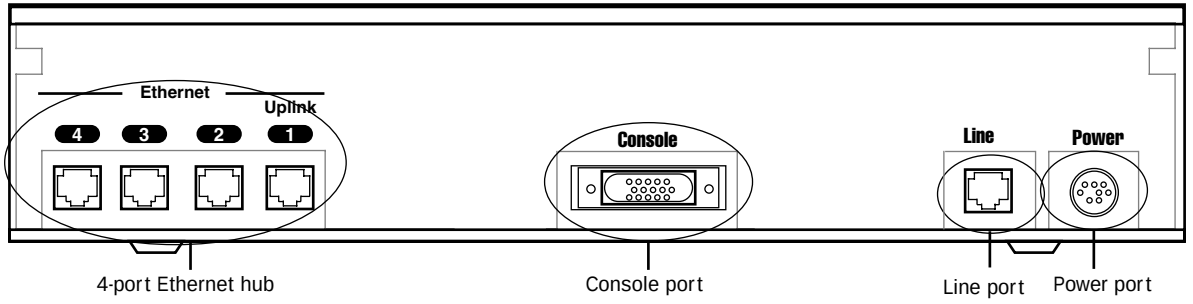
Once the Netopia R310 is properly configured and connected to your LAN, PC and Macintosh computers that have their required components in place will be able to connect to the Internet or other remote IP networks.

Connecting to an Ethernet network

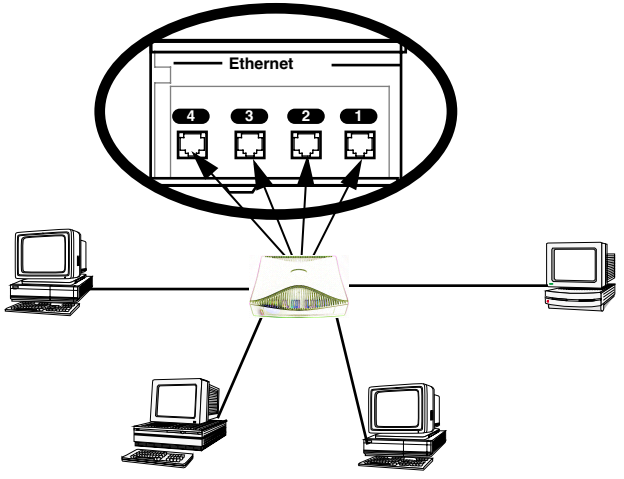
You can connect the Netopia R310 to an IP network that uses Ethernet. The Netopia R310 supports Ethernet connections through its four Ethernet ports. The Router automatically detects which Ethernet port is in use.

You can connect a standard 10Base-T Ethernet network to the Netopia R310 using any of its available Ethernet ports.

Netopia R310 back panel



The Netopia R310 in a 10Base-T network



To connect your 10Base-T network to the Netopia R310 through an Ethernet port, use a 10Base-T cable with RJ-45 connectors.

If you have more than four devices to connect, you can attach additional devices using a 10Base-T hub.

Chapter 5

Console-based Management

This chapter describes how to use the Console-based management screens on your Netopia R310 ISDN Router. The console screens provide an alternate method for experienced users to configure their router without using SmartStart. After completing the Easy Setup console screens, your router will be ready to connect to the Internet or another remote site.

This chapter covers the following topics:

About Console-based Management

Console-based management is a menu-driven interface for the capabilities built in to the Netopia R310. Console-based management provides access to a wide variety of features that the router supports. You can customize these features for your individual setup. This section describes how to access the console-based management screens.

Console-based management screens contain seven entry points to the Netopia Router configuration and monitoring features. The entry points are displayed in the Main Menu shown below:

```
                          Netopia R310 v4.6

                    Easy Setup...
                    WAN Configuration...
                    System Configuration...
                    Utilities & Diagnostics...
                    Statistics & Logs...
                    Quick Menus...
                    Quick View...
You always start from this main screen.
```

Note about screen differences. Netopia R310 models offering different feature sets will have variations in the fields on certain screens. For example, there are switched (dial-up ISDN) and leased (Synchronous/Asynchronous and T1) line models, as well as models that offer feature subsets such as SmartIP (Network Address Translation and DHCP). Your own console screens may look different from those illustrated in this manual.

- The **Easy Setup** menus display and permit changing the values contained in the default Connection Profile you created when you ran the SmartStart Wizard for initial configuration. Experienced users can also use Easy Setup to initially configure the router directly through a console session without using SmartStart.

  Easy Setup menus contain up to five descendant screens for viewing or altering these values. The number of screens depends on whether you have optional features installed.

- The **WAN Configuration** menu displays and permits changing your Connection Profile(s), creating or deleting additional Connection Profiles, and configuring or reconfiguring the manner in which you may be using the router to connect to more than one service provider or remote site.

- The **System Configuration** menus display and permit changing:
  - Network Protocols Setup. See "IP Setup and Network Address Translation" on page 9-1.
  - Filter Sets (Firewalls). See "Security" on page 12-1.
  - IP Address Serving. See "IP Setup and Network Address Translation" on page 9-1.
  - Date and Time. See "Date and Time" on page 7-13.
  - Console Configuration. See "Connecting a local terminal console cable to your router" on page 5-3.
  - SNMP (Simple Network Management Protocol). See "SNMP" on page 11-10.
  - Security. See "Security" on page 12-1.
  - Upgrade Feature Set. See "Upgrade Feature Set" on page 7-15.
  - Logging. See "Logging" on page 7-15.

- The **Utilities & Diagnostics** menus provide a selection of seven tools for monitoring and diagnosing the router's behavior, as well as updating the firmware and rebooting the system. See "Utilities and Diagnostics" on page 13-1 for detailed information.

- The **Statistics & Logs** menus display nine sets of tables and device logs that show information about your router, your network and their history. See "Statistics & Logs" on page 11-4 for detailed information.

- The **Quick Menus** screen is a shortcut entry point to many of the most commonly used configuration menus that are accessed through the other menu entry points.

- The **Quick View** menu displays at a glance current real-time operating information about your router. See "Quick View status overview" on page 11-1 for detailed information.

Connecting through a Telnet session

Features of the Netopia R310 may be configured through the console screens.

Before you can access the console screens through Telnet, you must have:

- a network connection locally to the router or IP access to the router through the WAN port. This could be the same connection as the one you used with SmartStart and the "Easy" path. If you used the default configuration for SmartStart, your IP address will be 192.168.1.1.

Note: Alternatively, you can have a direct serial console cable connection using the provided console cable for your platform (PC or Macintosh) and the "Console" port on the back of the router. For more information on attaching the console cable, see "Connecting a local terminal console cable to your router," below.

- **Telnet** software installed on the computer you will use to configure the router

Configuring Telnet software

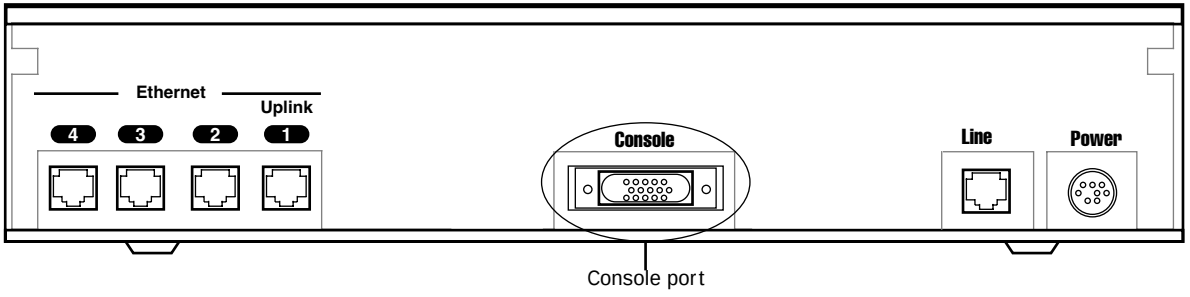
If you are configuring your router using a Telnet session, your computer must be running a Telnet software program.

- If you connect a PC with Microsoft Windows, you can use a Windows Telnet application or simply run Telnet from the Start menu.
- If you connect a Macintosh computer, you can use the NCSA Telnet program supplied on the Netopia R310 CD. You install NCSA Telnet by simply dragging the application from the CD to your hard disk.

Connecting a local terminal console cable to your router

You can perform all of the System Configuration activities for your Netopia R310 through a local serial console connection using terminal emulation software, such as HyperTerminal provided with Windows 95 or 98 on the PC, or ZTerm, included on the Netopia CD, for the Macintosh.

The Netopia R310 back panel has a connector labeled "Console" for attaching the Router to either a PC or Macintosh computer via the serial port on the computer. (On a Macintosh, the serial port is called the Modem port or the Printer port.) This connection lets you use the computer to configure and monitor the Netopia R310 via the console screens.



To connect the Netopia R310 to your computer for serial console communication, use the supplied dual console cable connector end appropriate to your platform:

- one DB-9 connector end attaches to a PC
- the mini-DIN8 connector end attaches to a Macintosh
- the DB-9 end of the Console cable attaches to the Netopia R310's Console port

If you are configuring your router via a *terminal* session, your computer must be running a standard terminal emulation or communications software program, such as those used with modems.

- If you connect a PC with Microsoft Windows 95 or NT, you can use the HyperTerminal application bundled

with the operating system.

- If you connect a Macintosh computer, you can use the ZTerm terminal emulation program on the supplied Netopia R310 CD.

Launch your terminal emulation software and configure the communications software for the following values. These are the default communication parameters that the Netopia R310 uses.

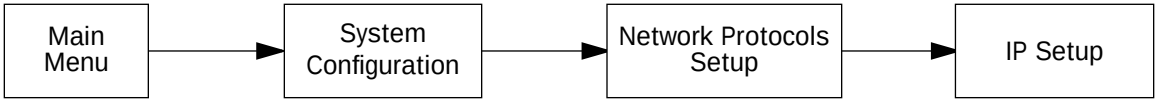
Parameter	Suggested Value
Terminal type	**PC**: ANSI-BBS **Mac**: ANSI, VT-100, or VT-200
Data bits	8
Parity	None
Stop bits	1
Speed	Options are: 9600, 19200, 38400, or 57600 bits per second
Flow Control	None
Note: The router firmware contains an autobaud detection feature. If you are at any screen on the serial console, you can change your baud rate and press Return (HyperTerminal for the PC requires a disconnect). The new baud rate is displayed at the bottom of the screen.	

Navigating through the console screens

Use your keyboard to navigate the Netopia R310's configuration screens, enter and edit information, and make choices. The following table lists the keys to use to navigate through the console screens.

To...	Use These Keys...
Move through selectable items in a screen or pop-up menu	Up, Down, Left, and Right Arrow
To set a change to a selected item or open a pop-up menu of options for a selected item like entering an upgrade key	Return or Enter
Change a toggle value (Yes/No, On/Off)	Tab
Restore an entry or toggle value to its previous value	Esc
Move one item up	Up arrow or Control + k
Move one item down	Down arrow or Control + j
Display a dump of the device event log	Control + e
Display a dump of the WAN event log	Control + f
Refresh the screen	Control + L
Go to topmost selectable item	<
Go to bottom right selectable item	>

To help you find your way to particular screens, some sections in this guide begin with a graphical path guide similar to the following example:



This particular path guide shows how to get to the Network Protocols Setup screens. The path guide represents these steps:

1. Beginning in the Main Menu, select the **System Configuration** item and press Return.
2. Select the **Network Protocols** item in the System Configuration screen and press Return.
3. Select the **IP Setup** item in the Network Protocols Setup screen and press Return.

To go back in this sequence of screens, use the Escape key.

Chapter 6

Easy Setup

This chapter describes how to use the Easy Setup console screens on your Netopia R310 ISDN Router. The Easy Setup console screens provide an alternate method for experienced users to set up their router's Connection Profiles without using SmartStart. After completing the Easy Setup console screens, your router will be ready to connect to the Internet or another remote site.

This chapter covers the following topics:

Easy Setup console screens

Using four Easy Setup console screens, you can:

- set up your switch type and datalink parameters
- create or modify a Connection Profile for your Router for the connection to your ISP or remote location
- set up IP addresses and IP address serving
- password protect configuration access to your Netopia R310 ISDN Router

How to access the Easy Setup console screens

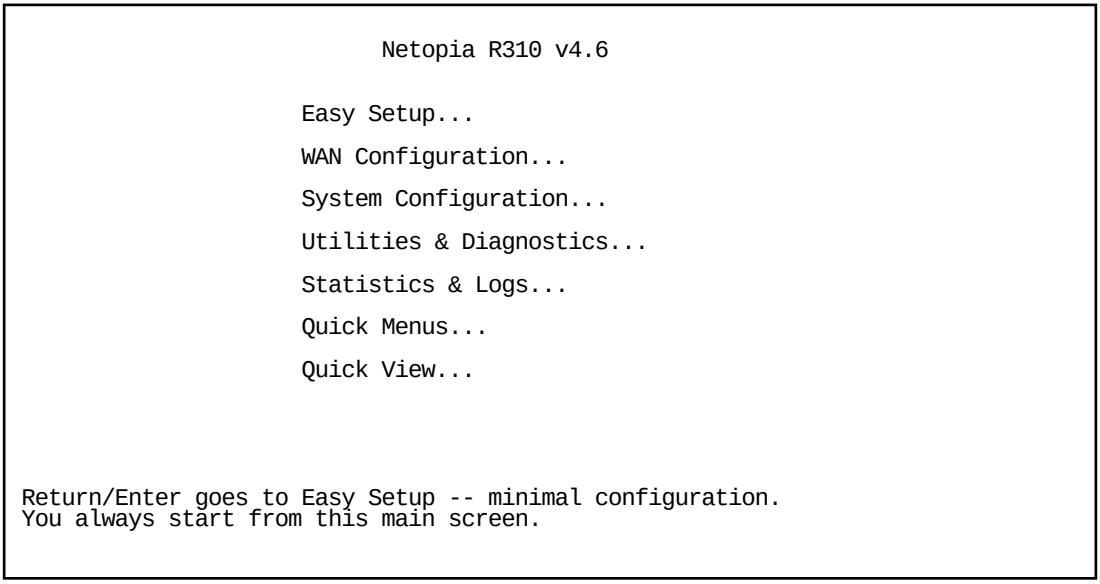
To access the console screens, Telnet to the Netopia Router over your Ethernet network, or you can physically connect with a serial console cable and access the Netopia Router with a terminal emulation program. See "Connecting through a Telnet session" on page 5-2 or "Connecting a local terminal console cable to your router" on page 5-3.

Note: Before continuing, make sure that you have the information that your telephone service provider, ISP, or network administrator has given you to configure the Netopia Router.

The Netopia Router's first console screen, Main Menu, appears in the terminal emulation window of the attached PC or Macintosh when:

- the Netopia Router is turned on
- the computer is connected to the Netopia Router
- the Telnet or terminal emulation software is running and configured correctly.

A screen similar to the following appears:



If you do not see the Main Menu, verify that:

- the computer used to view the console screen has its serial port connected to the Netopia R310's "Console" port or an Ethernet connection to one of its Ethernet ports. See "Connecting a local terminal console cable to your router" on page 5-3 or "Connecting through a Telnet session" on page 5-2.
- the Telnet or terminal emulation software is configured for the recommended values.
- if you are connecting via the Console port, the console's serial port is not being used by another device, such as an internal modem, or an application. Turn off all other programs (other than your terminal emulation program) that may be interfering with your access to the port.
- you have entered the correct password, if necessary. Your Netopia R310's console access may be password protected from a previous configuration. See your system administrator to obtain the password.

  See Appendix A, "Troubleshooting," for more suggestions.

Beginning Easy Setup

To begin Easy Setup, select **Easy Setup** in the Main Menu, then press Return.

The Easy Setup screen appears. **EuroISDN / ETSI**

```
                              ISDN Easy Setup


         Circuit Type...                    ISDN, Switched
         Switch Type...                     EuroISDN/ETSI          Detected

         Directory Number 1:                5088324614             Detected
         Directory Number 2:                5088324615             Detected

         PBX Prefix:

         Data Link Encapsulation...         PPP




         TO MAIN MENU                       NEXT SCREEN

Return/Enter to select <among/between> ...
Enter information supplied to you by your ISDN phone company.
```

ISDN Easy Setup

The Easy Setup Profile screen is where you configure the parameters that control the Netopia R310's connection to a specific remote destination, usually an ISP or a corporate site.

On a Netopia R310 ISDN Router you can add up to 15 more connection profiles, for a total of 16.

1. Select **Circuit Type** and press Return. From the pop-up menu, select:

   ISDN, Switched if you have a switched ISDN line. This option covers the broadest range of applications and defaults to Euro-ISDN, or

   ISDN, Leased if you have a dedicated or leased ("nailed-up") ISDN line that uses a single B channel (64K), 2B (128K), or the entire ISDN bandwidth of 2B+D (144K)

   If you select ISDN, Leased as your circuit type, select **Data Rate (kbps)**. From the pop-up menu, select the appropriate B-channel, such as B1, B2, B1+B2, or 2B+D. Then skip to step 6.

   It is possible to configure the router for any available circuit type: **ISDN, Switched** or **ISDN, Leased** depending on the switch gear you are connected to.

   If you create a connection profile using a particular datalink encapsulation method, that profile will take precedence whenever you connect to a line that uses that datalink encapsulation. If there is no connection profile with the datalink encapsulation method that the line uses, the router will default to using the default profile. See "The Default Profile" on page 7-5 for more information.

2. Select **Switch Type** and press Return. From the pop-up menu, select the switch protocol your ISDN service provider uses.

   For European countries other than the United Kingdom, use the **EuroISDN / ETSI** setting. United Kingdom users select **United Kingdom - EuroISDN**.

3. Select **Directory Number 1.**

   The router attempted to detect your Directory Number(s) when you selected Auto-Detect in Step 1.

   If it succeeded, the directory number(s) will be displayed, and the screen will indicate "Detected" (as shown on page 6-3).

   If it failed to detect your directory numbers, the fields will remain blank, and you must enter the primary directory number as you would dial it, including area code. Do not enter access prefixes such as Centrex or PBX prefixes like "9" (for an outside line). Press Return.

4. If you have a second directory number, select **Directory Number 2** and enter the secondary directory number as you would dial it, including area code. Press Return.

5. If you require a dialing prefix such as "9" to access an outside line on a PBX or Centrex phone system, select **PBX Prefix** and enter your dialing prefix. Press Return.

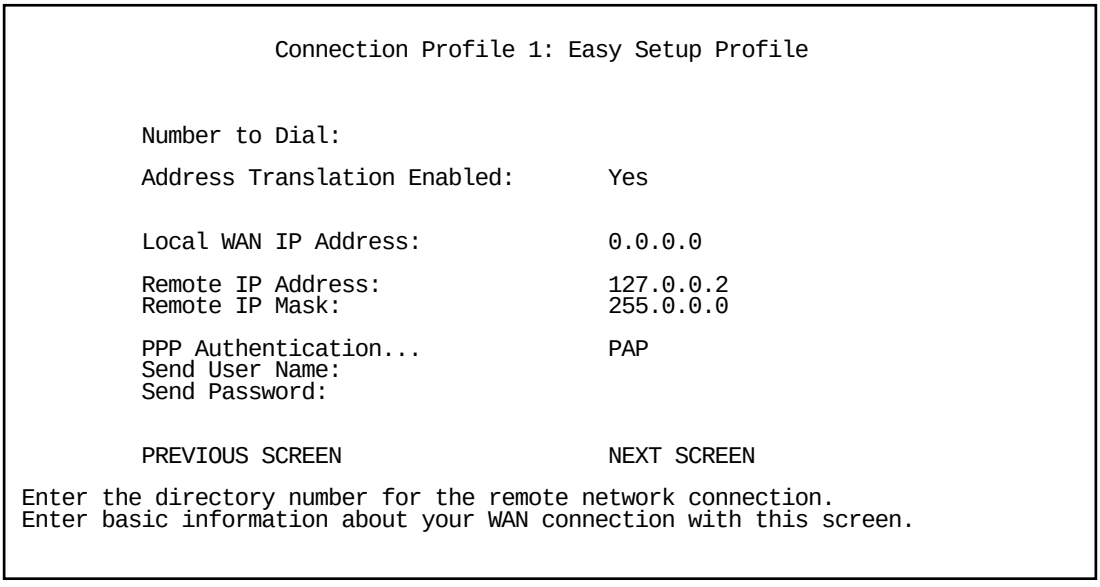
6. Select **Data Link Encapsulation** and highlight the method of encapsulation that you want to use from the pop-up menu. The choices offered are PPP or HDLC. The default for switched interfaces is PPP. Press Return.

7. Select **NEXT SCREEN** and press Return. The "Easy Setup Profile" screen (shown on page 6-5) appears.

Any changes you make to the ISDN configuration now or in the future will take effect immediately. You do not have to restart the router.

Easy Setup Profile

The Easy Setup Connection Profile screen is where you configure the parameters that control the ISDN Netopia Router's connection to a specific remote destination, usually another network.



1. Select **Number to Dial** and enter the ISDN telephone number you received from your ISP. This is the number the Netopia R310 dials to reach your ISP. Enter the number as you would dial it, including any required prefixes (such as area, access, and long-distance dialing codes).

   If you selected ISDN or Leased as your router's Circuit Type in the ISDN Easy Setup screen, Number to Dial will not be an available option.

2. To enable address translation, toggle **Address Translation Enabled** to **Yes**. For more information on Network Address Translation, see Chapter 9, "IP Setup and Network Address Translation."

   Then select the **Local WAN IP Address** field. The default address is 0.0.0.0, which allows for dynamic addressing, your ISP assigning an address each time you connect. However, you may enter another address if you want to use static addressing.

   Note: When using HDLC datalink encapsulation and Network Address Translation, you must use a static address.

3. If your ISP uses Numbered (Interface-based Routing), select **Local WAN IP Address** and enter the local WAN address your ISP gave you.

   When using numbered interfaces, the Netopia Router will use its local WAN IP address and subnet mask to send packets to the remote router. Both routers have WAN IP addresses and subnet masks associated with the connection.

   If your ISP uses Unnumbered (System-based Routing), select **Remote IP Address** and enter the IP address your ISP gave you. Then select **Remote IP Mask** and enter the IP subnet mask of the remote site you will connect to.

When using unnumbered interfaces, the Netopia Router will use either its local Ethernet IP address or its NAT address (if so configured) and subnet mask to send packets to the remote router. Neither router has a WAN IP address or subnet mask associated with this connection.

Note: If your ISP has not given you their IP or subnet mask addresses, then you may enter an IP address such as 127.0.0.2, and an IP subnet mask such as 255.0.0.0. which are acceptable as defaults values, and will typically be assigned at the time of connection.

4. **For circuits with PPP enabled:** Select the **PPP Authentication** pop-up menu and choose the type of connection security your ISP told you to use (either **None**, **PAP**, **CHAP**, **PAP-TOKEN**, or **CACHE-TOKEN**). If you choose **PAP**, **CHAP**, **PAP-TOKEN**, or **CACHE-TOKEN**, go to the next step. If your ISP does not use any of these authentication methods, choose **None** and skip to the last step. When you create a connection profile from Easy Setup, the default setting is PAP.

5. **For circuits with PPP enabled:** If your ISP uses PAP, select **Send User Name** and enter the user name your ISP gave you to connect. Then select **Send Password** and enter the password.

   If your ISP uses CHAP, select **Send Host Name** and enter the user name your ISP gave you to connect. Then select **Send Secret** and enter the secret (CHAP term for password) your ISP gave you.

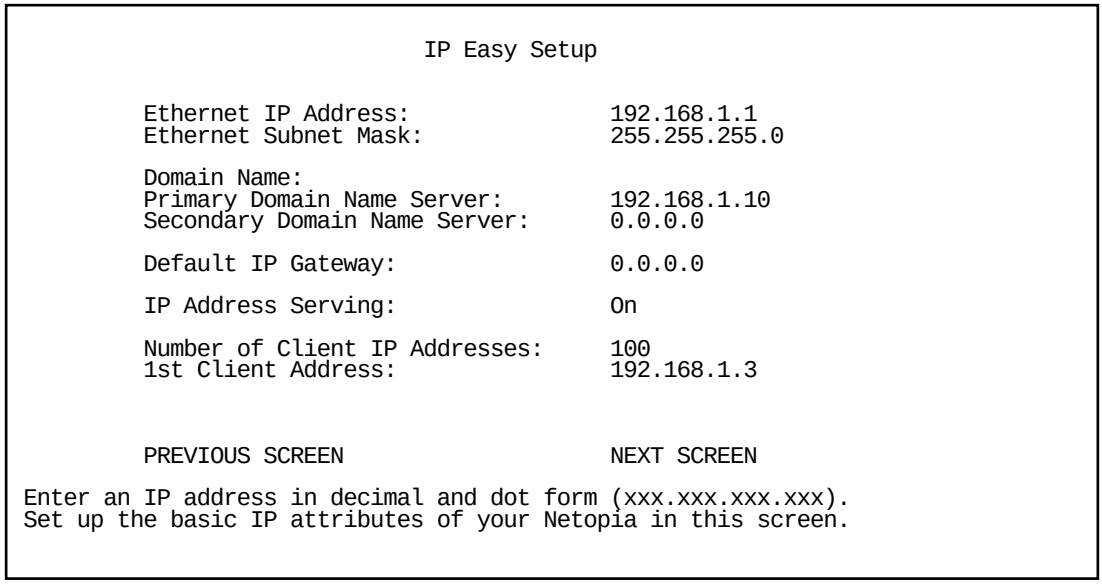
6. Select **NEXT SCREEN** and press Return. The IP Easy Setup screen appears.

IP Easy Setup

The IP Easy Setup screen is where you enter information about your Netopia Router's:

- IP address
- Subnet mask
- Default gateway IP address
- Domain name server IP address
- IP address serving information, such as the number of client IP addresses and the 1st client address; and

You should consult with your network administrator to obtain the information you will need. For more information about setting up IP, see "IP Setup and Network Address Translation" on page 9-1.



1. Select **Ethernet IP Address** and enter the first IP address from the IP address range your ISP has given you. This will be the Netopia Router's IP address.

   If Network Address Translation is enabled in the Easy Setup connection profile, the Ethernet IP Address defaults to an address within a range reserved by the Internet address administration authority for use within private networks, 192.168.1.1.

   Because this is a private network address, it should never be directly connected to the Internet. Using NAT for all your connection profiles will ensure this restriction. See "IP Setup and Network Address Translation" on page 9-1 for more information.

2. Select **Ethernet Subnet Mask** and enter the subnet mask your ISP has given you. The **Ethernet Subnet Mask** defaults to a standard class C mask, 255.255.255.0.
3. Select **Domain Name** and enter the domain name your ISP has given you.
4. Select **Primary Domain Name Server** and enter the IP address your ISP has given you.

5. The **Default IP Gateway** defaults to the remote IP address you entered in the Easy Setup connection profile. If the Netopia Router does not recognize the destination of any IP traffic, it forwards that traffic to this gateway – set to 127.0.0.2 if your ISP does not otherwise specify.

   Do not confuse the remote IP address and the default gateway's IP address with the block of local IP addresses you receive from your ISP. You use the local IP addresses for the Netopia R310's Ethernet port and for IP clients on your local network. The remote IP address and the default gateway's IP address should point to your ISP's router.

6. To use DHCP address serving, toggle **IP Address Serving** to **On**.

7. If **IP Address Serving** is **On**, select **Number of Client IP Addresses**. Then enter the number of available host addresses for the Netopia R310 ISDN Router to allocate to the client computers on your network. This number defaults to the balance of the subnet addresses above the Netopia Router's address.

8. If **IP Address Serving** is **On**, select **1st Client Address** and enter the first IP address in the set of allocated served IP addresses.

   Note: On a Netopia R310 the factory default IP Address serving settings are:

   1st Client Address: 192.168.1.3

   Number of Client IP Addresses: unlimited models:100; limited models: number of users minus 1

   (this allows for one static address at 192.168.1.2 for the server)

   The values you set in this screen are displayed in the "Quick View status overview" on page 11-1.

9. Press Return. The Easy Setup Security Configuration screen appears.

Easy Setup Security

The Easy Setup Security Configuration screen lets you password-protect your Netopia R310. Input your Write Access Name and Write Access Password with names or numbers totaling up to eleven digits.

If you password protect the console screens, you will be prompted to enter the name and password you have specified every time you log in to the console screens. Do not forget your name and password. If you do, you will be unable to access any of the configuration screens.

Additional security features are available. See Chapter 12, "Security."

```
                    Easy Setup Security Configuration

It is strongly suggested that you password-protect configuration access to your
Netopia. By entering a Name and Password pair here, access via serial, PC Card,
Telnet, SNMP and Web Server will be password-protected.

Be sure to remember what you have typed here, because you will be prompted for
it each time you configure this Netopia.


         Write Access Name:

         Write Access Password:



         PREVIOUS SCREEN       TO MAIN MENU      RESTART DEVICE

Configure a Configuration Access Name and Password here.
```

The final step in configuring the Easy Setup console screens is to restart the Netopia R310, so the configuration settings take effect.

1. Select **RESTART DEVICE**. A prompt asks you to confirm your choice.
2. Select **CONTINUE** to restart the Netopia Router and have your selections take effect.

Note: You can also restart the system at any time by using the restart utility (see “Restarting the system” on page 13-12) or by turning the Netopia Router off and on with the power switch.

Easy Setup is now complete.

Part II: Advanced Configuration

Chapter 7

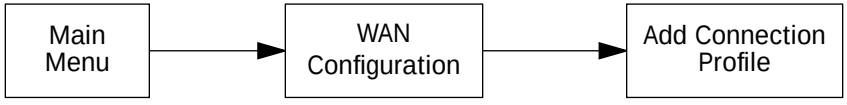
WAN and System Configuration

This chapter describes how to use the console-based management screens to access and configure advanced features of your Netopia R310 ISDN Router. You can customize these features for your individual setup. These menus provide a powerful method for experienced users to set up their router's connection profiles and system configuration.

This section covers the following topics:

Creating a new Connection Profile

Connection Profiles define the telephone and networking protocols necessary for the router to make a remote connection. A Connection Profile is like an address book entry describing how the router is to get to a remote site, or how to recognize and authenticate a remote user dialing in to the router. For example, to create a new **Connection Profile**, you navigate to the **WAN Configuration** screen from the Main Menu, and select Add Connection Profile.



The **Add Connection Profile** screen appears.

```
                          Add Connection Profile

        Profile Name:                     Profile 02
        Profile Enabled:                  Yes

        IP Enabled:                       Yes
        IP Profile Parameters...


        Data Link Encapsulation...        PPP
        Data Link Options...


        Telco Options...



        ADD PROFILE NOW                   CANCEL

Return accepts * ESC cancels * Left/Right moves insertion point * Del deletes.
Configure a new Conn. Profile. Finished?  ADD or CANCEL to exit.
```

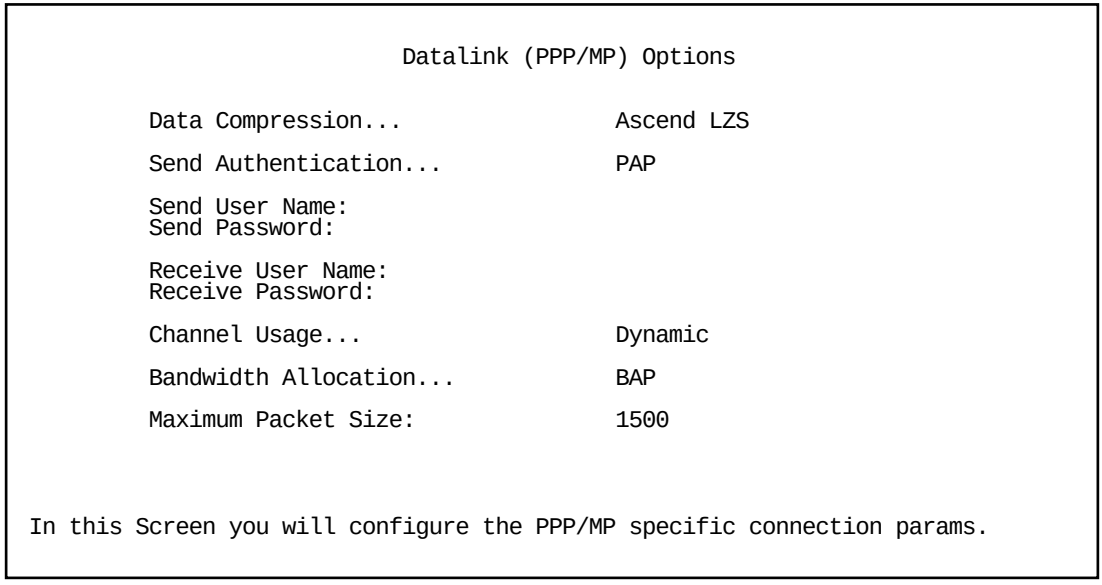
On a Netopia R310 ISDN Router you can add up to 15 more connection profiles, for a total of 16.

1. Select **Profile Name** and enter a name for this connection profile. It can be any name you wish. For example: the name of your ISP.
2. Toggle the **Profile Enabled** value to Yes or No. The default is Yes.
3. Select **IP Profile Parameters** and press Return. The IP Profile Parameters screen appears.

```
                          IP Profile Parameters


        Address Translation Enabled:      Yes


        Local WAN IP Address:             0.0.0.0

        Remote IP Address:                0.0.0.0
        Remote IP Mask:                   0.0.0.0

        Filter Set...
        Remove Filter Set

        Receive RIP:                      Off




Toggle to Yes if this is a single IP address ISP account.
Configure IP requirements for a remote network connection here.
```

4. Toggle or enter any IP Parameters you require and return to the Add Connection Profile screen by pressing Escape. For more information, see "IP Setup and Network Address Translation" on page 9-1.

5. Select **Datalink Options** and press Return. The Datalink Options screen appears.



You can accept the defaults, or change them if you wish. You can also specify user name and password for both outgoing and incoming calls. the Send User Name/Password parameters are used to specify your identity when dialing out to a remote location. The Receive User Name/Password parameters are used when receiving dial-in clients such as via RAS configuration.

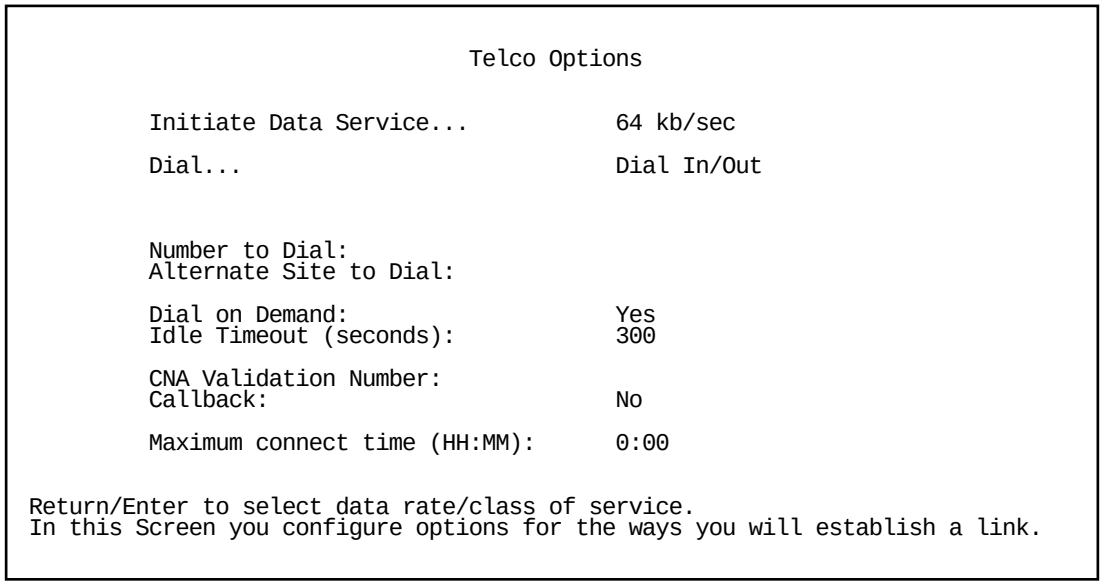
The **Channel Usage** pop-up menu allows you to choose how many lines your connections may use, and whether or not they are preemptable. Supported options are:

Option	Behavior
Dynamic	1 to 3 channels, if available, will be used, depending on traffic volume
1-Channel	Only 1 channel will be used
2-Channels	2 channels will be preferred
2-Channel Preemptable	2 channels will be used, but 1 may be reallocated

Note: The **Bandwidth Allocation** pop-up options are: Off, Auto, BAP or MP+. BAP is the default. You should only choose one of the other options if you are specifically advised to do so by your ISP or administrator.

Return to the Add Connection Profile screen by pressing Escape.

6. Select **Telco Options** and press return. the Telco Options screen appears.



Select **Dial** and press Return. A pop-up menu appears. You can select the dialing options for this Connection Profile as Dial In Only, Dial Out Only, or Dial In/Out.

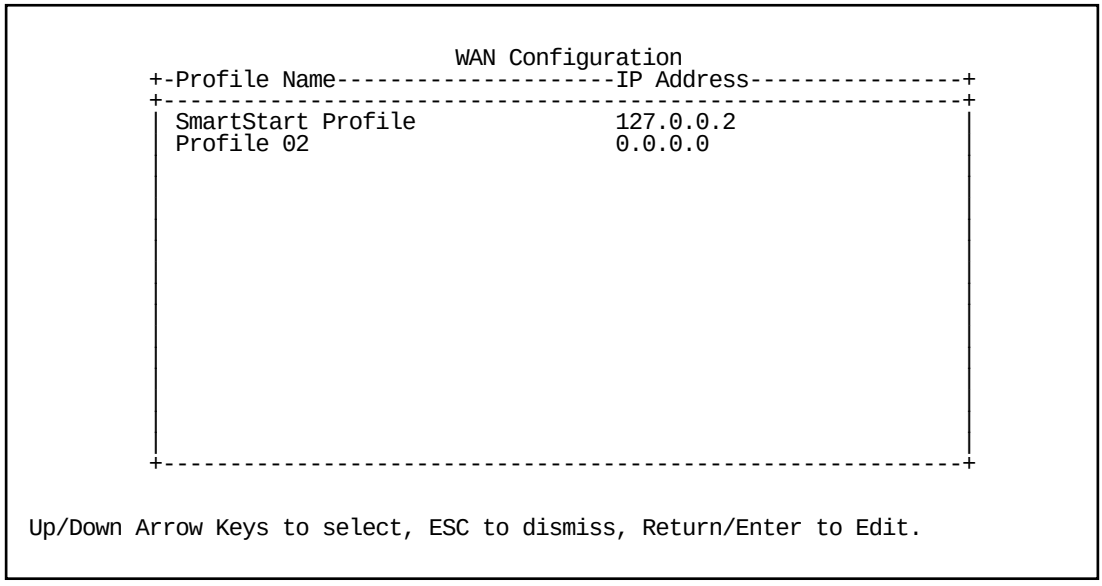
You can:

- select a type of data service to initiate, 64 kb/sec (the default), 56 kb/sec, or Speech
- add the number to dial for this Connection Profile
- add an alternate number
- change any of the default parameter settings
- if you have enabled Call Accounting (see "Cost control feature -- call accounting" on page 8-1) you can set the **Maximum connect time** for this connection profile by entering the hours and minutes in HH:MM format. When aggregate usage for this profile reaches this threshold, the profile becomes temporarily disabled until the limit is raised or the counters are reset (see "Viewing call accounting statistics" on page 8-2). If Call Accounting is not enabled, this field does not appear.

When you are finished with these entries, press Escape to return to the **Add Connection Profile** screen.

7. Select **ADD PROFILE NOW** and press Return. Your new Connection Profile will be added.

If you want to view the Connection Profiles in your router, return to the WAN Configuration screen, and select **Display / Change Connection Profile**. The list of Connection Profiles is displayed in a scrolling pop-up screen.



It is possible to configure the router for any available circuit type: **ISDN, Switched** or **ISDN, Leased**, depending on the switch gear you are connected to.

If you create a Connection Profile using a particular datalink encapsulation method, that profile will take precedence whenever you connect to a line that uses that datalink encapsulation. If there is no Connection Profile with the datalink encapsulation method that the line uses, the router will default to using the Default Profile. See “The Default Profile,” for more information.

The Default Profile

How the default profile works

The default profile works like a guard booth at the gate to your network: it scrutinizes WAN connections. Like the guard booth, the default profile allows connections based on a set of criteria that you define.

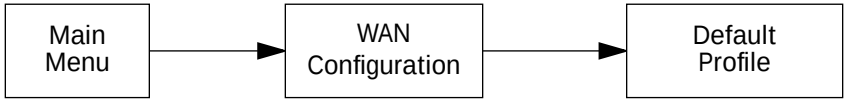
The main criterion used to check connections is whether they match one of the connection profiles already defined. A connection is matched to a connection profile using the remote network’s IP address (that is, the caller is defined as the destination of a particular connection profile).

If a connection matches an existing profile, all of the connection profile parameters are adopted for the call. When using PPP or Cisco-HDLC datalink encapsulation on a permanent circuit, you must configure a connection profile. Note, that you may have already configured this connection profile in Easy Setup.

See “Easy Setup” on page 6-1 for information on configuring an Easy Setup connection profile.

Customizing the Default Profile

The Default Profile screen controls whether or not an ISDN link will come up without an explicitly configured connection profile. See "Creating a new Connection Profile" on page 7-1 for more information. You access the Default Profile screen from the Main Menu by selecting WAN Configuration and then selecting **Default Profile**.



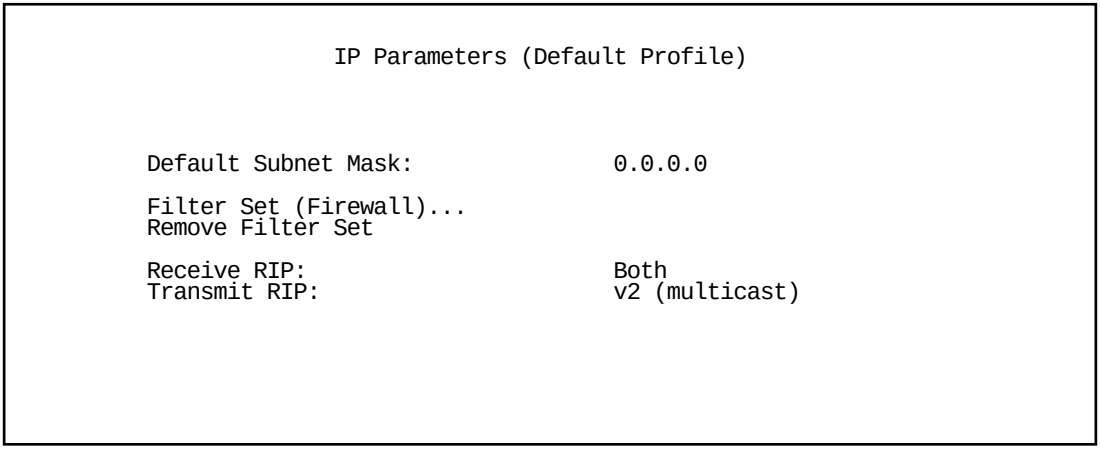
The Default Profile screen appears.

```
                          Default Profile

Must Match a Defined Profile:      Yes

IP Enabled:                        Yes
IP Parameters...
```

- You can set Must Match a Defined Profile item to Yes or No (the default). This item controls whether or not the ISDN link will come up without an explicitly configured connection profile. If your ISP is serving you a dynamic IP Address, you need not explicitly configure a connection profile, and the default behavior of the router will be to connect automatically once it is powered on.
- If Must Match a Defined Profile is set to No, then an IP Enabled item is visible. Toggling this item to Yes (the default) or No controls whether or not IP will be supported on the ISDN link. If IP Enabled is set to Yes, an IP Parameters item becomes visible. If you select IP Parameters the IP Parameters screen appears (see "IP parameters (default profile) screen" on page 7-7). This screen allows you to configure various IP parameters for ISDN connections established without an explicitly configured connection profile.

IP parameters (default profile) screen

The IP Parameters (Default Profile) screen allows you to configure various IP parameters for ISDN connections established without an explicitly configured connection profile:



The Netopia R310 ISDN Router always acts as a DHCP client on the ISDN link when using a Default Profile. The DHCP server will supply a local IP address and subnet mask. For an ISDN link, Network Address Translation (NAT) is enabled by default in the Default Profile and the Default Subnet Mask is set to 0.0.0.0. For details on setting up IP Parameters see “IP Setup and Network Address Translation” on page 9-1.

Routing Information Protocol (RIP) is needed if there are IP routers on other segments of your Ethernet network that the Netopia R310 needs to recognize. Set to “Both” (the default) the Netopia R310 will accept information from either RIP v1 or v2 routers. Alternatively, select **Receive RIP** and select **v1** or **v2** from the popup menu. With Receive RIP set to “v1,” the Netopia R310’s Ethernet port will accept routing information provided by RIP packets from other routers that use the same subnet mask. Set to “v2,” the Netopia R310 will accept routing information provided by RIP packets from other routers that use different subnet masks.

If you want the Netopia R310 to advertise its routing table to other routers via RIP, select **Transmit RIP** and select **v1**, **v2 (broadcast)**, or **v2 (multicast)** from the popup menu. With Transmit RIP v1 selected, the Netopia R310 will generate RIP packets only to other RIP v1 routers. With Transmit RIP v2 (broadcast) selected, the Netopia R310 will generate RIP packets to all other hosts on the network. With Transmit RIP v2 (multicast) selected, the Netopia R310 will generate RIP packets only to other routers capable of recognizing RIP v2 packets.

```
                    IP Parameters (Default Profile)

          Default Subnet Mask:               0.0.0.0



          Filter Set (Firewall)...
          Remove Filter Set

          Receive RIP:                     +------------------+
          Transmit RIP:                    +------------------+
          TX RIP Policy...                 | Poison Reverse   |
                                           | Split Horizon    |
                                           | No Split Horizon |
                                           +------------------+
```

If you choose to transmit RIP, the TX RIP Policy pop up menu appears. You can select **Poison Reverse** (the default), **Split Horizon**, or **No Split Horizon**.

- Poison Reverse speeds convergence but adds to network overhead. When topology changes, mentioning routes that should not go through the router as well as those that should can speed up convergence.
- If you select Split Horizon ("without Poison Reverse" is implied), the router omits routes learned from an interface from RIP updates sent on that interface. Split Horizon without Poison Reverse has the advantage of minimizing network overhead in large network configurations at the expense of slower convergence.
- No Split Horizon is suitable for partially meshed networks. A partially meshed network is a WAN in which one or more nodes do not have logically direct connections to all other nodes. In a star or partially meshed topology, you may need to disable Split Horizon so the routers can learn about other networks.

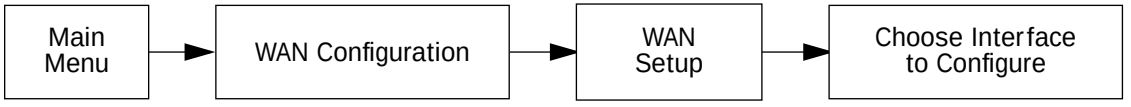
Delayed Remote Configuration Change Toggle

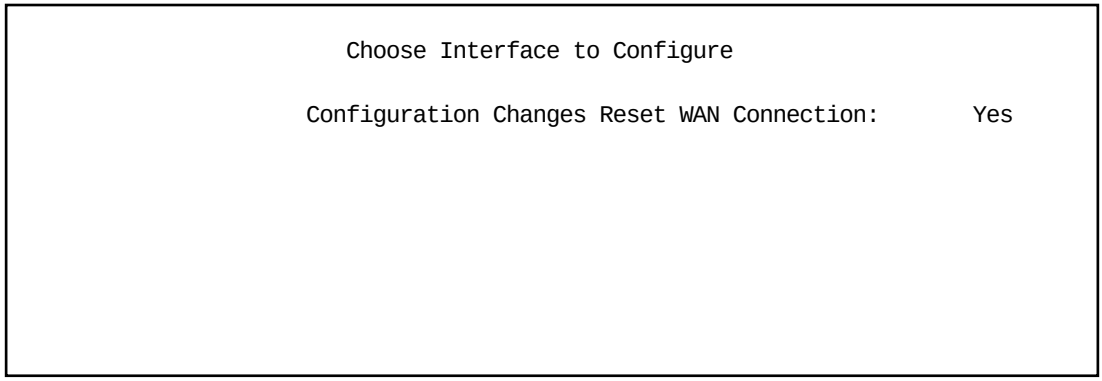
The Netopia R310 supports delaying some configuration changes until after the router is restarted.

If your router is preconfigured by your service provider, or if you are not remotely configuring the router, you can leave this setting unchanged.

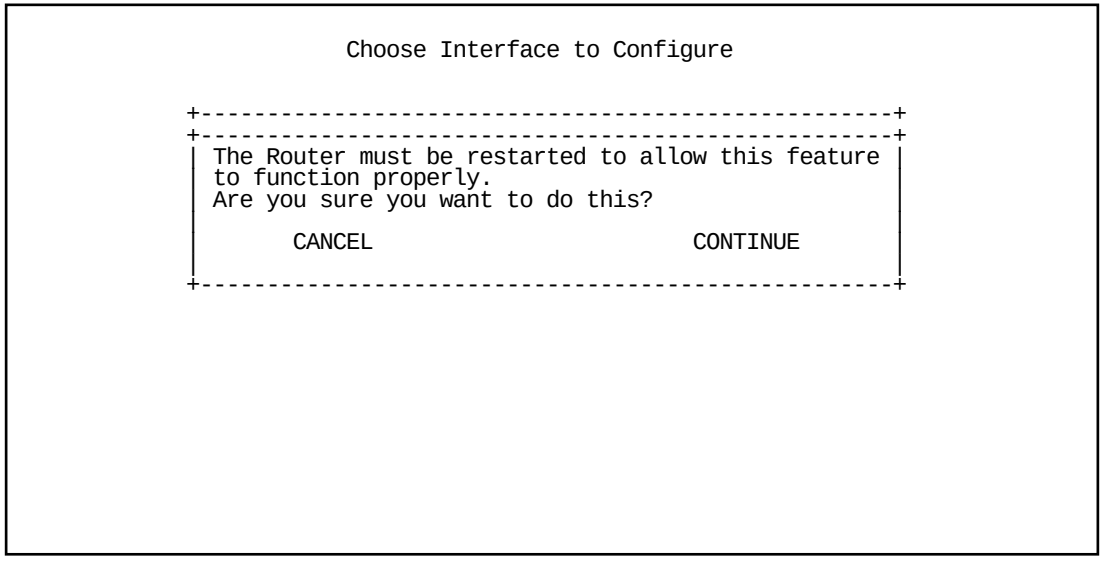
The purpose of this feature is to defer configuration changes *only* when remotely configuring or reconfiguring the router to prevent premature console disconnection. When this feature is enabled, no changes to the WAN setup, datalink encapsulation, Connection Profiles, DLCIs, or Default Gateways will take effect until after the router is restarted. Until the router is restarted the WAN link and the routing table remain unaffected.

A single setting in the **Choose Interface to Configure** screen controls this feature, as shown below.





When you toggle **Configuration Changes Reset WAN Connection** using the Tab key and press **Return**, a pop-up window asks you to confirm your choice.



Toggling from **Yes** to **No** makes the router ready to be configured. If you toggle from **No** to **Yes**, and confirm the reboot, your changes are committed and the router comes up using the newly created configuration.

System Configuration screens

```
                          ISDN Line Configuration

         Circuit Type...                    ISDN, Switched
         Switch Type...                     AT&T 5ESS Pt-to-Pt

         Directory Number 1:                555-1234



         PBX Prefix:

         Data Link Encapsulation...         PPP

         Data Rate (kbps)...                38.4


Return/Enter to select <among/between> ...
Enter information supplied to you by your ISDN phone company.
```

You can connect to the Netopia R310's System Configuration screens:

- Using Telnet with the Router's Ethernet port IP address
- Through the console port, using a local terminal (see "Connecting a local terminal console cable to your router" on page 5-3)

You can also retrieve the Netopia R310's configuration information and remotely set its parameters using the Simple Network Management Protocol (see "SNMP" on page 11-10).

Open a Telnet connection to the IP address you set in the router with SmartStart, for example "192.168.1.1."

The console screen will open to the **Main Menu**, similar to the screen shown below:

```
                          Netopia R310 v4.6

                      Easy Setup...
                      WAN Configuration...
                      System Configuration...
                      Utilities & Diagnostics...
                      Statistics & Logs...
                      Quick Menus...
                      Quick View...
Return/Enter goes to Easy Setup -- minimal configuration.
You always start from this main screen.
```

System Configuration features

SmartStart may be all you need to configure your Netopia R310. Some users, however, require advanced settings or prefer manual control over the default selections that SmartStart automatically chooses. For these users, the Netopia R310 provides System Configuration options.

To help you determine whether you need to use the System Configuration options, review the following requirements. If you have one or more of these needs, use the System Configuration options described in the later chapters.

- Two or more outgoing connection profiles to connect to more than one remote location (for example, to connect to the Internet and to a network at another office).
- System Configuration of dynamic IP address distribution through DHCP, MacIP, or BootP.
- Customized incoming call profile to control received calls.
- Scheduled connections.
- Greater network security through the use of filters, CallerID, callback, and SecurID.
- System Configuration of connection profiles. See the table below for a partial list of the options available through System Configuration.

Layer Category	Parameter Type	Options	Default settings
Protocol Layer	IP Parameters	Filter Sets:	Basic Firewall
		RIP Receive/Transmit options:	Off
Datalink Layer	PPP/MP Parameters	Data Compression:	Ascend LZS
		Send Authentication:	PAP
		Channel Usage:	Dynamic
		Bandwidth Allocation:	BAP
		Maximum Packet Size:	1500
Physical Layer	Telco Parameters	Dial is set to:	Dial In/Out
		Dial On Demand is set to:	Yes
		Callback is set to:	No
		Idle Time-out is set for:	300 seconds

To access the System Configuration screens, select **System Configuration** in the Main Menu, then press Return.

The System Configuration screen appears:

```
                        System Configuration

                    Network Protocols Setup...
                    Filter Sets (Firewalls)...
                    IP Address Serving...

                    Date and Time...

                    Console Configuration...

                    SNMP (Simple Network Management Protocol)...

                    Security...

                    Upgrade Feature Set...

                    Telephone Setup...

                    Logging...

Return/Enter to configure Networking Protocols (such as TCP/IP).
Use this screen if you want options beyond Easy Setup.
```

Network Protocols Setup

These screens allow you to configure your network's use of IP.

- Details are given in "IP Setup and Network Address Translation" on page 9-1.

Filter Sets (Firewalls)

These screens allow you to configure security on your network by means of filter sets and a basic firewall.

- Details are given in "Security" on page 12-1.

IP Address Serving

These screens allow you to configure IP Address serving on your network by means of DHCP, WANIP, and BootP.

- Details are given in "IP Setup and Network Address Translation" on page 9-1.

Date and Time

You can set the system's date and time in the **Set Date and Time** screen.

Select **Date and Time** in the System Configuration screen and press Return to go to the Set Date and Time screen.

```
                          Set Date and Time

System Date Format:                          MM/DD/YY
Current Date (MM/DD/YY):                     3/16/1998

System Time Format:                          AM/PM
Current Time:                                10:29
AM or PM:                                    AM
```

Follow these steps to set the system's date and time:

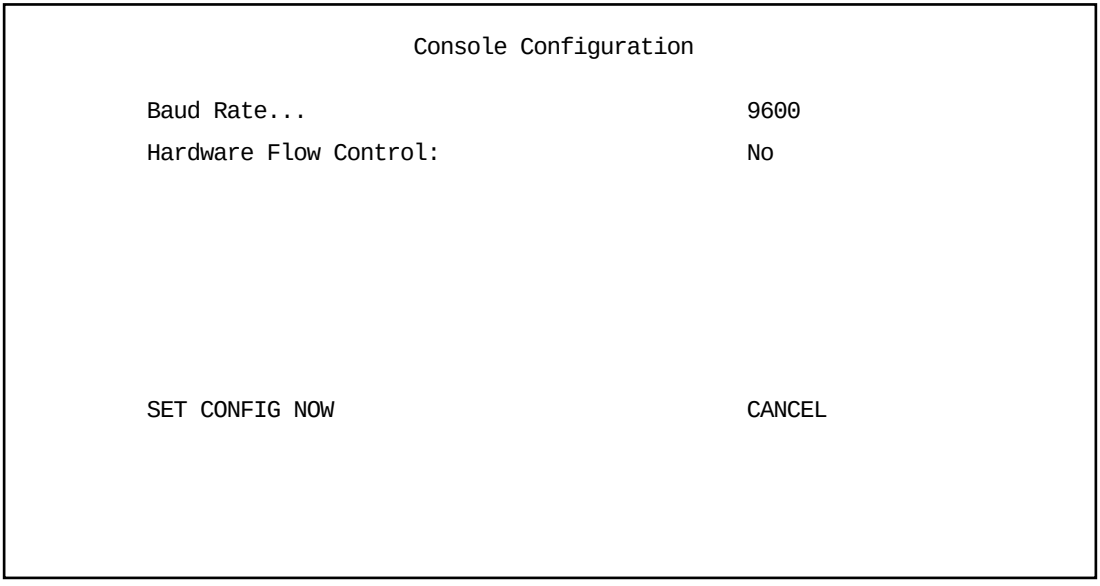
1. Select **Current Date** and enter the date in the appropriate format. Use one- or two-digit numbers for the month and day, and the last two digits of the current year. The date's numbers must be separated by forward slashes (/).
2. Select **Current Time** and enter the time in the format HH:MM, where HH is the hour (using either the 12-hour or 24-hour clock) and MM is the minutes.

3. Select **AM or PM** and choose **AM** or **PM**.

Console Configuration

You can change the default terminal communications parameters to suit your requirements.

To go to the Console Configuration screen, select **Console Configuration** in the System Configuration screen.



Follow these steps to change a parameter's value:

1. Select the parameter you want to change.
2. Select a new value for the parameter. Return to step 1 if you want to configure another parameter.
3. Select **SET CONFIG NOW** to save the new parameter settings. Select **CANCEL** to leave the parameters unchanged and exit the Console Configuration screen.

SNMP (Simple Network Management Protocol)

These screens allow you to monitor and configure your network by means of a standard Simple Network Management Protocol (SNMP) agent.

- Details are given in “SNMP” on page 11-10.

Security

These screens allow you to add users and define passwords on your network.

- Details are given in “Security” on page 12-1.

Upgrade Feature Set

You can upgrade your Netopia R310 by adding new feature sets through the **Upgrade Feature Set** utility.

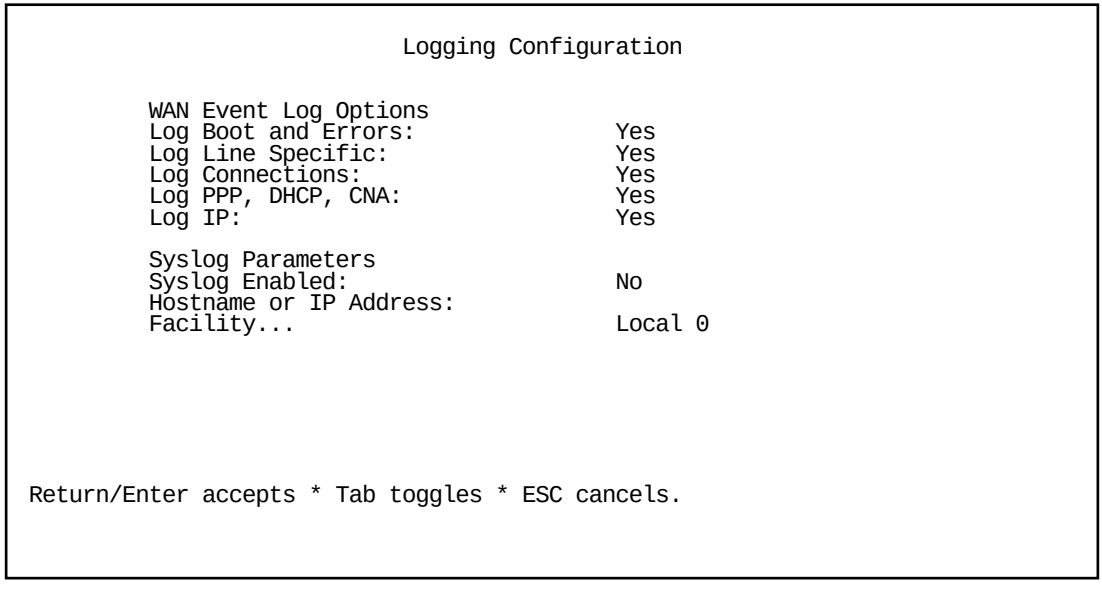
Vvisit the Netopia Web site at www.netopia.com for information on new feature sets, how to obtain them, and how to install them on your Netopia R310.

Logging

You can configure a UNIX-compatible syslog client to report a number of subsets of the events entered in the router’s WAN Event History. See “WAN Event History” on page 11-6.

Select **Logging** from the System Configuration menu.

The Logging Configuration screen appears.



By default, all events are logged in the event history.

- By toggling each event descriptor either **Yes** or **No**, you can determine which ones are logged and which are ignored.
- You can enable or disable the syslog client dynamically. When enabled, it will report any appropriate and previously unreported events.
- You can specify the syslog server's address either in dotted decimal format or as a DNS name up to 63 characters.
- You can specify the UNIX syslog Facility to use by selecting the **Facility** pop-up.

The following screen shows a sample syslog dump of WAN events:

```
Nov  5 10:14:06 tsnext.netopia.com   Link 1 down: PPP PAP failure
Nov  5 10:14:06 tsnext.netopia.com >>Issued Speech Setup Request from our DN: 5108645534
Nov  5 10:14:06 tsnext.netopia.com   Requested Disc. from DN: 917143652500
Nov  5 10:14:06 tsnext.netopia.com   Received Clear Confirm for our DN: 5108645534
Nov  5 10:14:06 tsnext.netopia.com   Link 1 down: Manual disconnect
Nov  5 10:14:06 tsnext.netopia.com >>Issued Speech Setup Request from our DN: 5108645534
Nov  5 10:14:06 tsnext.netopia.com   Requested Disc. from DN: 917143652500
Nov  5 10:14:06 tsnext.netopia.com   Received Clear Confirm for our DN: 5108645534
Nov  5 10:14:06 tsnext.netopia.com   Link 1 down: No answer
Nov  5 10:14:06 tsnext.netopia.com --Device restarted----------------------------------------
Nov  5 10:14:06 tsnext.netopia.com >>Received Speech Setup Ind. from DN: (not supplied)
Nov  5 10:14:06 tsnext.netopia.com   Requested Connect to our DN: 5108645534
Nov  5 10:14:06 tsnext.netopia.com   ASYNC: Modem carrier detected (more) Modem reports: 26400
V34
Nov  5 10:14:06 tsnext.netopia.com >>WAN: 56K Modem 1 activated at 115 Kbps
Nov  5 10:14:06 tsnext.netopia.com   Connect Confirmed to our DN: 5108645534
Nov  5 10:14:06 tsnext.netopia.com   PPP: Channel 1 up, Answer Profile name: Default Profile
Nov  5 10:14:06 tsnext.netopia.com    PPP: NCP up, session 1, Channel 1 Final (fallback)
negotiated auth: Local PAP , Remote NONE
Nov  5 10:14:06 tsnext.netopia.com   PPP: PAP  we accepted remote, Channel 1 Remote name: guest
Nov  5 10:14:06 tsnext.netopia.com    PPP: MP negotiated, session 1 Remote EDO: 06 03
0000C5700624 0
Nov  5 10:14:06 tsnext.netopia.com   PPP: CCP negotiated, session 1, type: Ascend LZS Local
mode: 1, Remote mode: 1
Nov  5 10:14:06 tsnext.netopia.com   PPP: BACP negotiated, session 1 Local MN: FFFFFFFF, Remote
MN: 00000001
Nov  5 10:14:06 tsnext.netopia.com  PPP: IPCP negotiated, session 1, rem: 192.168.10.100 local:
192.168.1.1
Nov  5 10:14:06 tsnext.netopia.com >>WAN: 56K Modem 1 deactivated
Nov  5 10:14:06 tsnext.netopia.com   Received Clear Ind. from DN: 5108645534, Cause: 0
Nov  5 10:14:06 tsnext.netopia.com   Issued Clear Response to DN: 5108645534
Nov  5 10:14:06 tsnext.netopia.com   Link 1 down: Remote clearing
Nov  5 10:14:06 tsnext.netopia.com   PPP: IPCP down, session 1
Nov  5 10:14:06 tsnext.netopia.com >>Received Speech Setup Ind. from DN: (not supplied)
```

Chapter 8

Call Accounting and Default Answer Profile

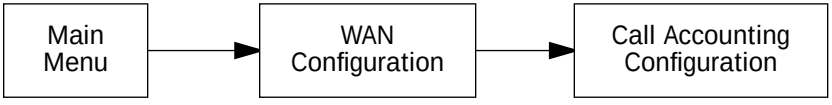
You can set a Netopia Router to make scheduled connections using designated connection profiles. This is useful for creating and controlling regularly scheduled periods when the router can be used by hosts on your network. It is also useful for once-only connections that you want to schedule in advance.

The Netopia R310 ISDN Router can also answer calls as well as initiate them. To answer calls, the Netopia R310 uses a Default Answer Profile. The Default Answer Profile controls how incoming calls are set up, authenticated, filtered, and more.

Topics in this chapter include:

Cost control feature -- call accounting

The Netopia R310 offers system-wide and per connection profile call accounting to track first minutes (an ISDN tariff factor) and additional minutes, for initiated data and voice calls.



To go to the Call Accounting screen, select **Call Accounting Configuration** in the WAN Configuration screen.

```
                    Call Accounting Configuration

          Enable Call Accounting:            On
          Day for auto-reset of timers:      12
          Maximum Aggregate connect time:    12:00
```

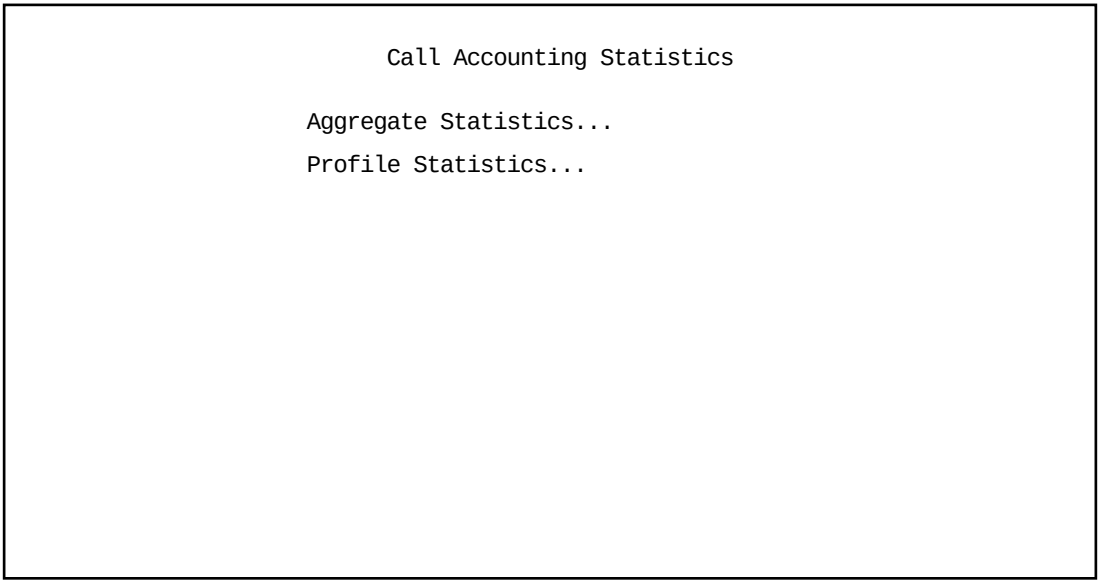
To enable call accounting, follow these steps:

1. Select **Enable Call Accounting** and toggle it to **On**.
2. Select **Day for auto-reset of timers** and enter the day of the month for the Router to reset the Call Accounting Statistics.
3. Select **Maximum Aggregate connect time (HH:MM)** and enter the total amount of time to allow for outbound calls, where HH is the hour (using either the 12-hour or 24-hour clock) and MM is the minutes.

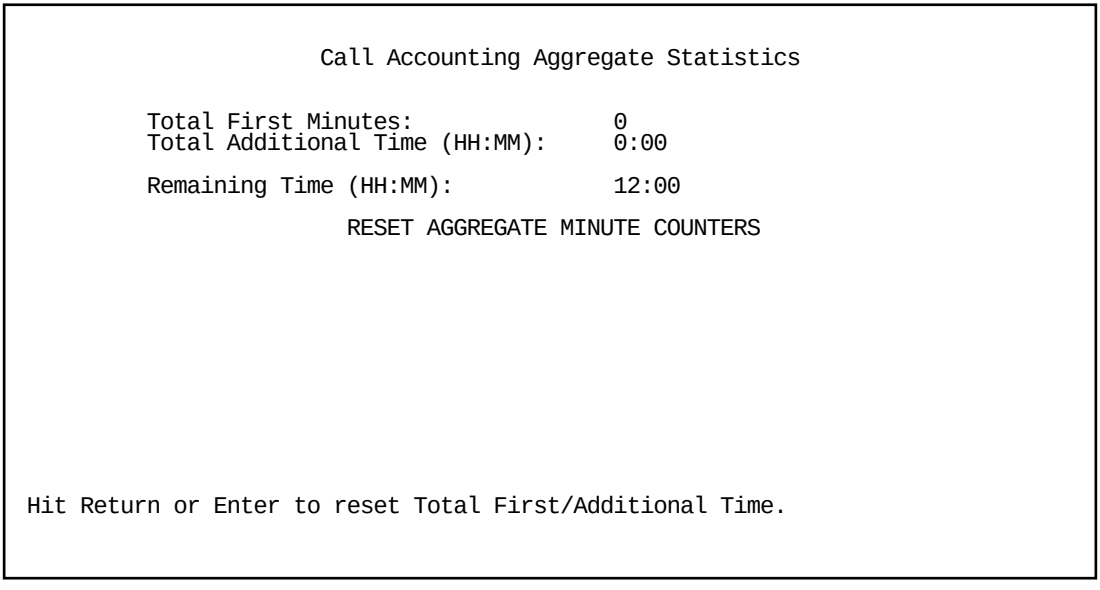
Viewing call accounting statistics

To view call accounting statistics, go to the Statistics & Logs screen from the Main Menu and select **Call Accounting Statistics**.

The Call Accounting Statistics screen appears.



If you select **Aggregate Statistics**, the following screen appears.



- **Total First Minutes** displays the total number of first minutes of outbound calls placed during the recording interval.
- **Total Additional Minutes (HH:MM)** displays the total remaining time of all outbound calls placed during the recording interval.
- **Remaining Time (HH:MM)** displays how much time is left in the recording interval. If call accounting is not enabled, the message will read, Call Accounting Disabled.

- You can reset the counters by selecting **RESET AGGREGATE MINUTE COUNTERS**. A dialog box will ask you to confirm the reset. Select **CONTINUE** to reset the counters or **CANCEL** to leave them as is.

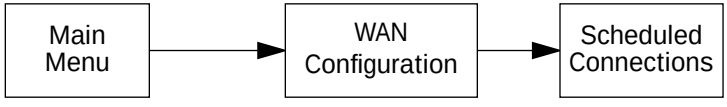
If you select **Profile Statistics**, the following screen appears.

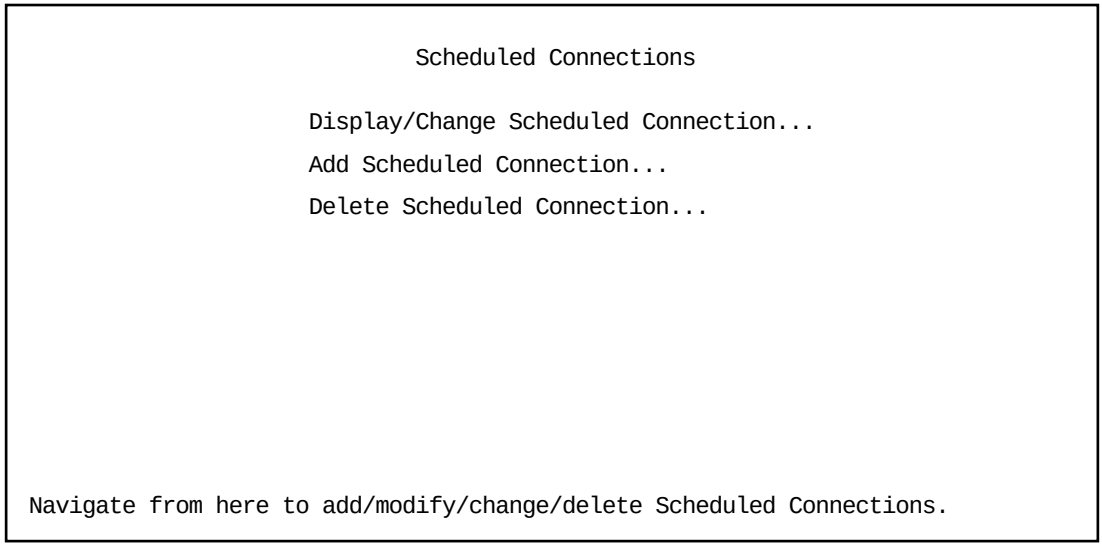
```
                Call Accounting Profile Statistics (in HHHH:MM)

Profile Name---------First Minutes----Additional Minutes-------Cutoff--Expired
---------------------------------SCROLL UP-----------------------------------
Easy Setup Profile            0:00                  0:00         0:00




---------------------------------SCROLL DOWN---------------------------------
```

You can view the individual usage statistics for each of the Connection Profiles you have defined.

Scheduled connections

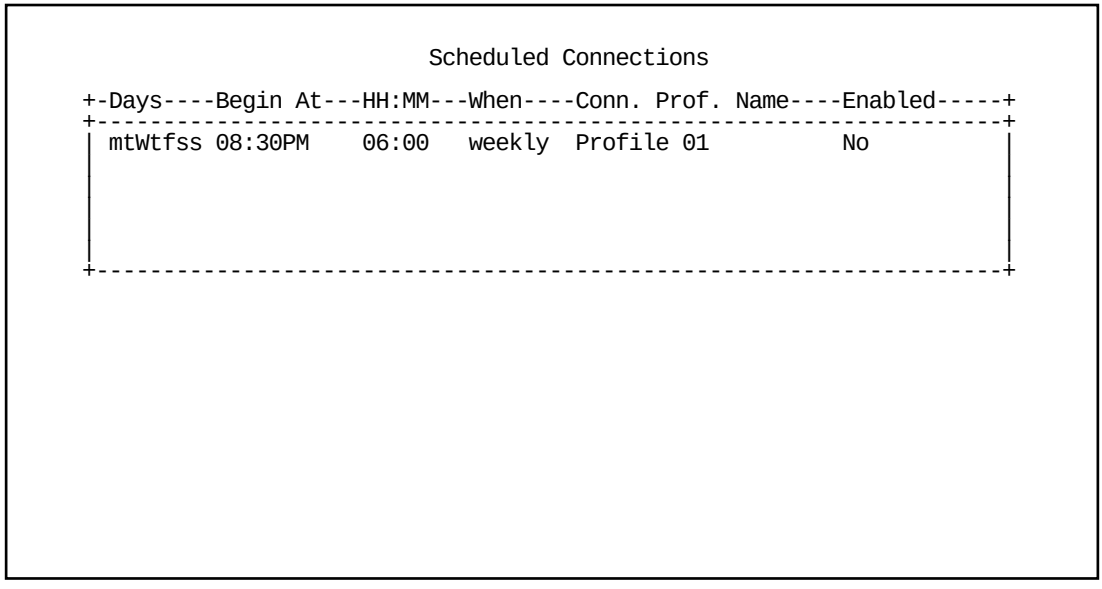
To go to the Scheduled Connections screen, select **Scheduled Connections** in the WAN Configuration screen.





Viewing scheduled connections

To display a table of view-only scheduled connections, select **Display / Change Scheduled Connection** in the Scheduled Connections screen. Each scheduled connection occupies one row of the table.



The first column in the table shows a one-letter representation of the **Days** of the week, from Monday (M or m) to Sunday (S or s). If a letter representing a day is capitalized, the connection will be activated on that day; a lower-case letter means that the connection will not be activated on that day. If the scheduled connection is configured for a once-only connection, the word “once” will appear instead of the days of the week.

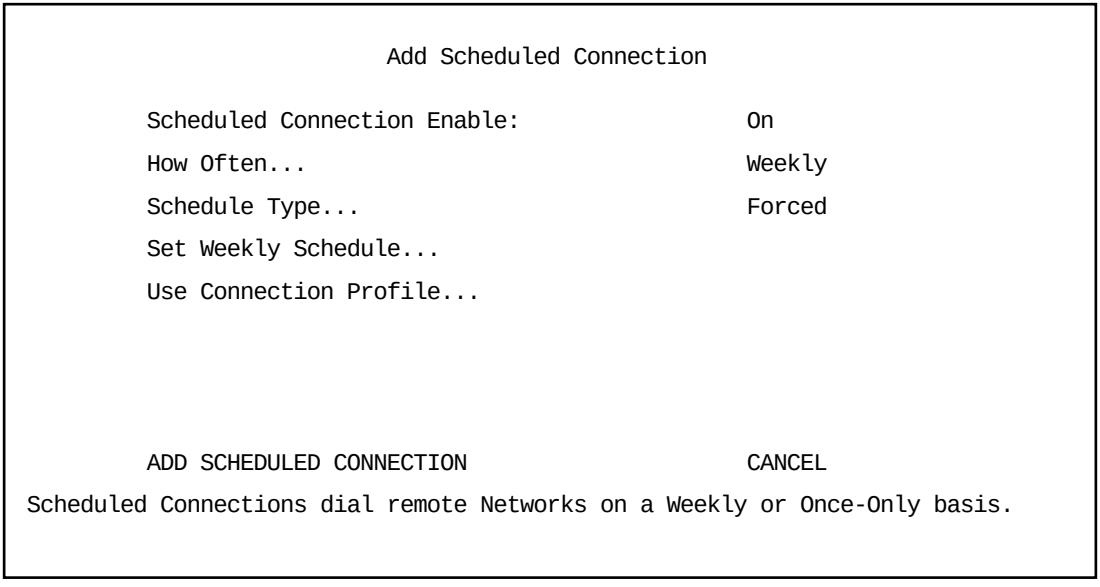
The other columns show:

- The time of day that the connection will **Begin At**
- The duration of the connection (**HH:MM**)
- Whether it's a recurring **Weekly** connection or used **Once Only**
- Which connection profile (**Conn. Prof.**) is used to connect
- Whether the scheduled connection is currently **Enabled**

The router checks the date and time set in scheduled connections against the system date and time.

Adding a scheduled connection

To add a new scheduled connection, select **Add Scheduled Connection** in the Scheduled Connections screen and press Return. The Add Scheduled Connection screen appears.



Follow these steps to configure the new scheduled connection:

- To activate the connection, select **Scheduled Connection Enable** and toggle it to **On**. You can make the scheduled connection inactive by toggling **Scheduled Connection Enable** to **Off**.
- Decide how often the connection should take place by selecting **How Often** and choosing **Weekly** or **Once Only** from the pop-up menu.
- The **Schedule Type** allows you to set the exact weekly schedule or once-only schedule.

  Options are:

  - **Forced Up**, meaning that this connection will be maintained whether or not there is a demand call on the line.
  - **Forced Down**, meaning that this connection will be torn down or blocked whether or not there is a demand call on the line.

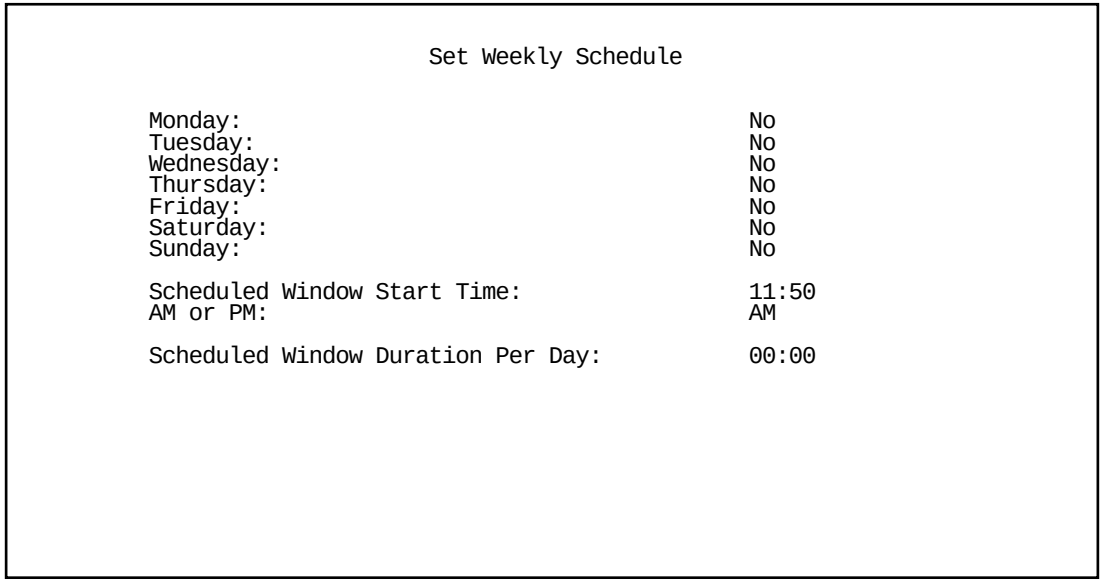
- **Demand-Allowed**, meaning that this schedule will permit a demand call on the line.
- **Demand-Blocked**, meaning that this schedule will prevent a demand call on the line.
- **Periodic**, meaning that the connection is retried several times during the scheduled time.

- If **How Often** is set to **Weekly**, the item directly below **How Often** reads **Set Weekly Schedule**. If **How Often** is set to **Once Only**, the item directly below **How Often** reads **Set Once-Only Schedule**.

Set Weekly Schedule

If you set **How Often** to **Weekly**, select **Set Weekly Schedule** and go to the Set Weekly Schedule screen.

- Select the days for the scheduled connection to occur and toggle them to **Yes**.

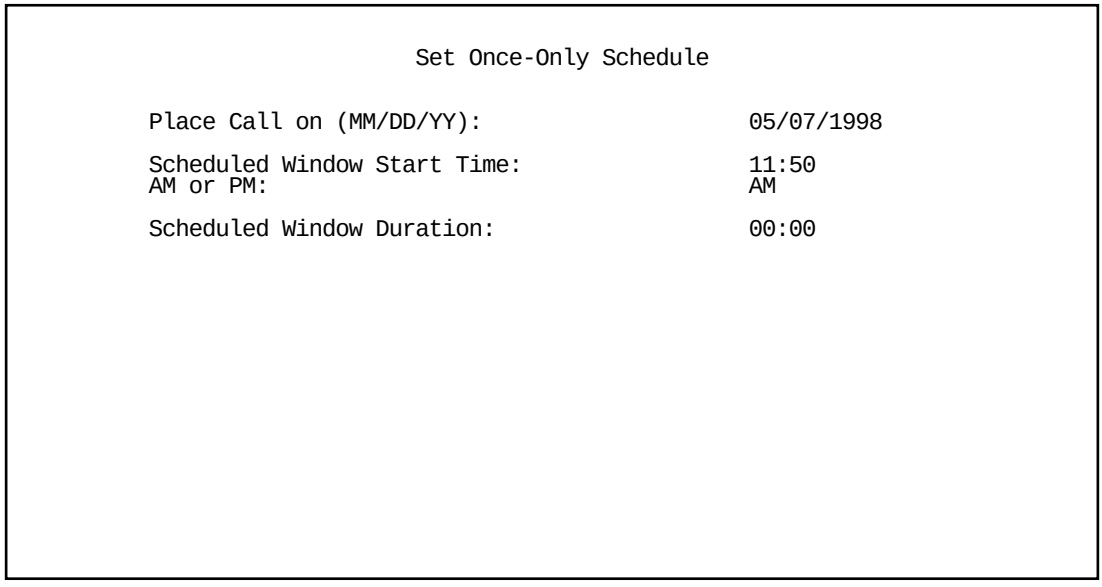


- Select **Scheduled Window Start Time** and enter the time to initiate the scheduled connection.
- You must enter the time in the format H:M, where H is a one- or two-digit number representing the hour and M is a one- or two-digit number representing the minutes. The colon is mandatory. For example, the entry 1:3 (or 1:03) would be accepted as 3 minutes after one o'clock. The entry 7:0 (or 7:00) would be accepted as seven o'clock, exactly. The entries 44, :5, and 2: would be rejected.
- Select **AM or PM** and choose **AM** or **PM** from the pop-up menu.
- Select **Scheduled Window Duration Per Day** and enter the maximum duration allowed for this scheduled connection, per call.

  You are finished configuring the weekly options. Return to the Add Scheduled Connection screen to continue.

Set Once-Only Schedule

If you set **How Often** to **Once Only**, select **Set Once-Only Schedule** and go to the Set Once-Only Schedule screen.



- Select **Place Call On (Date)** and enter a date in the format MM/DD/YY or MM/DD/YYYY (month, day, year).

  Note: You must enter the date in the format specified. The slashes are mandatory. For example, the entry 5/7/98 would be accepted as May 7, 1998. The entry 5/7 would be rejected.

- Select **Scheduled Window Start Time** and enter the time to initiate the scheduled connection.

  Note: You must enter the time in the format H:M, where H is a one- or two-digit number representing the hour and M is a one- or two-digit number representing the minutes. The colon is mandatory. For example, the entry 1:3 (or 1:03) would be accepted as 3 minutes after one o'clock. The entry 7:0 (or 7:00) would be accepted as seven o'clock, exactly. The entries 44, :5, and 2: would be rejected.

- Select **AM or PM** and choose **AM** or **PM**.

- Select **Scheduled Window Duration** and enter the maximum duration allowed for this scheduled connection. Use the same format restrictions noted above.

You are finished configuring the once-only options. Return to the Add Scheduled Connection screen to continue.

- In the Add Scheduled Connection screen, select **Use Connection Profile** and choose from the list of connection profiles you have already created. A scheduled connection must be associated with a connection profile to be useful. The connection profile becomes active during the times specified in the associated scheduled connection, if any exists.

- Select **ADD SCHEDULED CONNECTION** to save the current scheduled connection. Select **CANCEL** to exit the Add Scheduled Connection screen without saving the new scheduled connection.

Modifying a scheduled connection

To modify a scheduled connection, select **Change Scheduled Connection** in the Scheduled Connections screen to display a table of scheduled connections.

Select a scheduled connection from the table and go to the Change Scheduled Connection screen. The parameters in this screen are the same as the ones in the Add Scheduled Connection screen (except that **ADD SCHEDULED CONNECTION** and **CANCEL** do not appear). To find out how to set them, see "Adding a scheduled connection" on page 8-6.

Deleting a scheduled connection

To delete a scheduled connection, select **Delete Scheduled Connection** in the Scheduled Connections screen to display a table of scheduled connections.

Select a scheduled connection from the table and press the Return key to delete it. To exit the table without deleting the selected scheduled connection, press the Escape key.

Default Answer Profile

The Netopia R310 ISDN Router can answer calls as well as initiate them. To answer calls, the Netopia R310 uses a Default Answer Profile. The Default Answer Profile controls how incoming calls are set up, authenticated, filtered, and more.

How the Default Answer Profile works

The Default Answer Profile works like a guard booth at the gate to your network: it scrutinizes incoming calls. Like the guard booth, the Default Answer Profile allows calls based on a set of criteria that you define.

The main criterion used to check calls is whether they match one of the Connection Profiles already defined. If PAP or CHAP authentication is being used, the default profile checks that the incoming call's name and password/secret match the receive name and password/secret of a Connection Profile. If PAP or CHAP is not being used, an incoming call is matched to a Connection Profile using the remote network's IP address (that is, the caller is defined as the destination of a particular connection profile).

If an incoming call is matched to an existing Connection Profile, the call is accepted. All of that Connection Profile's parameters, except for authentication, are adopted for the call.

You could set up the Default Answer Profile to allow calls in even if they fail to match a Connection Profile. Continuing the guard booth analogy, this would be like removing the guards or having them wave all calls in, regardless of their source.

If an incoming call is not required to match a connection profile, and fails to do so, it is accepted as a standard IP connection. Accepted, unmatched calls adopt the call parameter values set in the Default Answer Profile.

To determine the call parameter values that unmatched calls will adopt, customize the Default Answer Profile parameters in the Default Answer Profile screen.

Customizing the default profile

You can customize the Netopia Router's default profile in the Default Answer Profile screen under the WAN Configuration menu.

1. Select **Default Answer Profile** in the WAN Configuration screen. Press Return. The Default Profile screen appears.

```
                          Default Answer Profile

          Calling Number Authentication...   Preferred
          Force 56k on Answer:               No

          Must Match a Defined Profile:      Yes









          PPP Authentication...              PAP
          Bandwidth Allocation...            BAP




 Configure values which may be used when receiving a call in this screen.
```

2. To enable CNA-authentication, select **Calling Number Authentication** in the Default Answer Profile screen and choose one of the following settings:

   Ignored: Calling Number Authentication (CNA) is not in effect.

   Preferred: This is the default setting. Authentication is attempted if the calling number is available. If authentication fails, or the calling number is not available, the call proceeds as usual and the caller may still connect successfully. Use this setting if you expect to receive both regular and CNA-authenticated calls.

   Required: Authentication is attempted if the calling number is available. If authentication fails, or the calling number is not available, the Netopia R310 disconnects the caller. Use this setting if you require all calls to be CNA-authenticated.

   Calling Number Authentication (CNA), is an application of CallerID. It is a method of verifying that an incoming call is originating from an expected site. Using CNA, you can increase the security of your network by requiring that callers not only possess the correct PPP authentication information, but also are calling from a particular physical location.

CNA works by checking the calling number that the Netopia Router receives during the initial setup phase of an incoming call against a set of stored numbers. Each number in the stored set is defined in a specific connection profile. When a match occurs, the incoming call is handled by the connection profile containing the matched number.

Using CNA can also provide cost savings because calls are not billed during the CNA phase. With CNA, a caller can set up a connection to the Netopia R310 without incurring any charges by accessing a dial-back connection profile. If the caller's rates are higher than those charged to the Netopia R310's return call, then using CNA has saved the difference.

CNA should be available where CallerID services are available. You will need to consult with your telephone service provider to find out if your line is provisioned for CallerID compliant with Bellcore specifications.

Also note that if the calling side has instructed the phone company to block delivery of its caller ID, the answering side will not be able to authenticate.

Notes:

- If your line does not support the appropriate service, CNA may not work properly.
- Certain European switch types do not pass a leading zero (0) in a directory number. If a caller is initiating a call from a number with a leading zero, and you have CNA set to include the leading zero, the connection may fail because the intervening telephone switch dropped the leading zero, and the calling number mismatches your entry. A workaround would be not to use the leading zero in your CNA Validation Number entry in the Telco Options screen. See the Telco Options screen on page 7-4.

3. To force a call to be answered at 56K, toggle **Force 56K on Answer** to **Yes**. Otherwise, the default will remain 64K.

4. To force incoming calls to match connection profiles, select **Must Match a Defined Profile** and toggle it to **Yes**. Incoming calls that cannot be matched to a connection profile are dropped. To allow unmatched calls to be accepted as standard IP connections, toggle **Must Match a Defined Profile** to **No**.

   If **Must Match a Defined Profile** is set to **Yes**, the answer profile only accepts calls that use the same authentication method defined in the **Authentication** item. If PAP or CHAP are involved, the caller must have a name and password or secret that match one of the connection profiles. The caller must obtain these from you or your network administrator before initiating the call.

   For example, if **Must Match a Defined Profile** is set to **Yes**, and **Authentication** is set to **PAP**, then only incoming calls that use PAP and match a connection profile will be accepted by the answer profile.

   If authentication in the Default Answer Profile is set to CHAP, the value of the **CHAP Challenge Name** item must be identical to the value of the **Send Host Name** item of the Connection Profile to be matched by the caller.

   If **Must Match a Defined Profile** is set to **No**, **Authentication** is assumed to be **None**, even if you've set it to **PAP** or **CHAP.** The answer profile uses the caller's IP address to match a connection profile. However, the answer profile cannot discover a caller's subnet mask; it assumes that the caller is *not* subnetting its IP address:

   Class A addresses are assumed to have a mask of 255.0.0.0

   Class B addresses are assumed to have a mask of 255.255.0.0

   Class C addresses are assumed to have a mask of 255.255.255.0. Class C address ranges are generally the most common subnet allocated.

If a remote network has a non-standard mask (that is, it uses subnetting), the only way for it to successfully connect to the Netopia Router is by matching a connection profile. In other words, you will have to set up a connection profile for that network.If **Must Match a Defined Profile** is set to **No**, you can also set the following parameters for accepted calls that do not match a connection profile:

Call acceptance scenarios

The following are a few common call acceptance scenarios and information on how to configure the Netopia R310 for those purposes.

- To accept all calls, regardless of whether they match a connection profile:
  - Toggle **Must Match a Defined Profile** to **No**.
- To only accept calls that match a connection profile through use of a name and password (or secret):
  - Toggle **Must Match a Defined Profile** to **Yes**, *and*
  - Set **Authentication** to **PAP** or **CHAP**.

  Note: The authentication method you choose determines which connection profiles are accessible to callers. For example, if you choose PAP, callers using CHAP or no authentication will be dropped by the answer profile.
- To allow calls that *only* match a connection profile's remote IP address:
  - Toggle **Must Match a Defined Profile** to **Yes**, *and*
  - set **Authentication** to **None**.
- To not allow *any* incoming calls to connect to the Netopia Router:
  - Toggle **Must Match a Defined Profile** to **Yes**, *and*
  - Set the **Dial** option in the Telco Options screen of every connection profile to **Dial Out Only**

5. If you select **Bandwidth Allocation**, you can select a value from a pop-up window. Supported options are Off, Auto, MP+, or BAP. The Bandwidth Allocation setting will apply to all answered calls.

   Note: The **Bandwidth Allocation** default is BAP. You should only choose one of the other options if you are specifically advised to do so by your ISP or administrator.

Chapter 9

IP Setup and Network Address Translation

The Netopia R310 uses Internet Protocol (IP) to communicate both locally and with remote networks. This chapter shows you how to configure the router to route IP traffic. You also learn how to configure the router to serve IP addresses to hosts on your local network.

Netopia's SmartIP features IP address serving and Network Address Translation. For a detailed discussion of Network Address Translation, see Appendix E, "Understanding Netopia NAT Behavior." This chapter describes how to use the Network Address Translation feature of SmartIP.

Note: When you configured your Netopia R310 using SmartStart, Network Address Translation was enabled by default. You have the option of disabling it, if you wish. This is done through the System Configuration screens using Console-based Management.

This section covers the following topics:

Network Address Translation Overview

NAT (Network Address Translation) is a means of mapping one or more IP addresses and/or IP service ports into different values. This *mapping* serves two functions:

- It allows the addresses of many computers on a LAN to be represented to the public Internet by only one or a few addresses, saving you money.
- It can be used as a security feature by obscuring the true addresses of important machines from potential hackers on the Internet.

To help you understand some of the concepts discussed here, it may be helpful to introduce some NAT terminology.

The term *mapping* refers to rules that associate one or more private addresses on the Netopia R310's LAN to one or more public addresses on the Netopia R310's WAN interface (typically the Internet).

The terms *private* and *internal* refer to addresses on the Netopia R310's LAN. These addresses are considered private because they are protected or obscured by NAT and cannot be directly accessed from the WAN (or Internet) side of the Netopia R310 unless specifically configured otherwise.

The terms *public* and *external* refer to the WAN (or Internet) side of the Netopia R310.

Features

MultiNAT features can be divided into several categories that can be used simultaneously in different combinations on a per-Connection Profile basis.

The following is a general description of these features:

Port Address Translation

The simplest form of classic Network Address Translation is *PAT* (Port Address Translation). PAT allows a group of computers on a LAN, such as might be found in a home or small office, to share a single Internet connection using one IP address. The computers on the LAN can surf the web, read email, download files, etc., but their individual IP addresses are never exposed to the public network. Instead, a single IP address, the IP address of the router, acts as the source IP address of traffic originating from the LAN. The Netopia allows you to define multiple PAT mappings, which can be individually mapped to different public IP addresses. This offers more control over the access permitted to users on the LAN.

A limitation of PAT is that communication must be initiated from the internal network. A user on the external side can not access a machine behind a PAT connection. A PAT feature is the ability to define multiple PAT mappings. Each of these can optionally map to a section or *range* of IP addresses of the internal network. PAT mapping allows only internal users to initiate traffic flow between the internal and external networks.

Server lists

Server lists, previously known as exported services, make it possible to provide access from the public network to hosts on the LAN. Server Lists allow you to define particular services, such as web, ftp, or e-mail, which are available via a public IP address. You define the type of service you would like to make available, and the internal IP address to which you would like to provide access. You may also define a specific public IP address to use for this service if you want to use an IP other than the WAN IP address of the Netopia R310.

Static mapping

If you want to host your own website or provide other Internet services to the public, you need more than classic NAT. The reason is noted above – external users cannot initiate traffic to computers on your LAN because external users can never see the real addresses of the computers on your LAN. If you want users outside your LAN to have access, for example, to a web or FTP server that you host, you need to make a representation of the real IP addresses of those servers public.

Static mappings are a way to make one or more private IP addresses fully accessible from the public network via corresponding public IP addresses. Some applications may negotiate multiple TCP connections in the process of communication, which often does not work with traditional PAT. Static mapping offers the ability to use these applications through NAT. Each private IP address is mapped, on a one-to-one basis, to a public IP address that can be accessed from the Internet or public network. As with PAT mappings, you may have multiple Static mappings to map a range of private IP addresses to a range of public IP addresses if desired.

Dynamic mapping

Dynamic mapping, often referred to as Many-to-Few, offers an extension to the advantages provided by Static mapping. Instead of requiring a one to one association of public addresses and private addresses, as is required in Static mapping, Dynamic mapping uses a group of public IP addresses to dynamically allocate static mappings to private hosts that are communicating with the public network. If a host on the private network initiates a connection to the Internet, for example, the Netopia R310 automatically sets up a one-to-one mapping of that host's private IP address to one of the public IP addresses allocated to be used for Dynamic NAT. As long as this host is communicating with the Internet, it will be able to use that address. When traffic from that host ceases, and no traffic is passed from that host for five minutes, the public address is made available again for other private hosts to use as necessary.

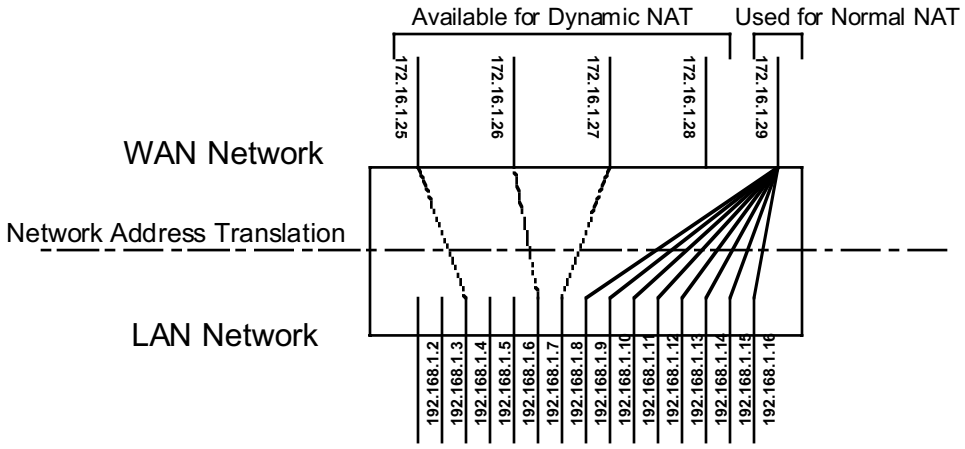
When addresses are returned to the group of available addresses, they are returned to the head of the group, being the most recently used. If that same host requests a connection an hour later, and the same public address is still available, then it will be mapped to the same private host. If a new host, which has not previously requested a connection, initiates a connection it is allocated the last, or oldest, public address available.

Dynamic NAT is a way of sharing a range of public, or exterior, NAT addresses among one or more *groups* of private, or interior, hosts. It is generally referred to as *Many-to-Few* mapping. This is intended to provide superior support for applications that traditionally have difficulty communicating through NAT. Dynamic NAT is intended to provide functionality beyond Many-to-One and One-to-One translation. Now it is possible to have a static mapping of one public address to one private address, thus allowing applications such as NetMeeting to work by assuring that any traffic sent back to the source IP address is forwarded through to the internal machine.

Static One-to-One mapping works well if you have enough IP addresses for all the workstations on your LAN. If you do not, Dynamic NAT allows machines to make full use of the publicly routable IP addresses provided by the ISP as necessary, on demand. When these public IP addresses are no longer being used by a particular workstation, they are returned to a pool of available addresses for other workstations to use.

A common example is a DSL customer's application. Most DSL ISPs only provide customers with a few IP addresses for use on their network. For networks with more than four or five machines it is usually mandatory to use NAT. A customer may have 15 workstations on the LAN, all of which need Internet access. The customer is only provided five IP addresses by their ISP. The customer has eight hosts, which only need to use email and have web access, but another seven hosts, which use NetMeeting to communicate with clients once or twice a day. NetMeeting will not work unless a static One-to-One mapping exists for the machine running NetMeeting to use for communication. The customer does not have enough IP addresses to create a One-to-One mapping for each of the seven users. This is where Dynamic NAT applies.

The customer can configure four of these addresses to be used for Dynamic NAT. The fifth address is then used for the eight other machines that do not need One-to-One mappings. As each machine configured to use addresses from the dynamic pool tries to connect to the Internet it is allocated a public IP address to use temporarily. Once the communication has been terminated, that IP address is freed for one of the other six hosts to use.



Exterior addresses are allocated to internal hosts on a demand, or as-needed, basis and then made available when traffic from that host ceases. Once an internal host has been allocated an address, it will use that address for all traffic. Five minutes after all traffic ceases – no pings, all tcp connections closed, no DNS requests, etc. – the address is put at the head of an *available* list. If an interior host needs an exterior address an hour later, and the previously used address is still available, it will acquire the same address. If an interior host that has not previously been allocated an exterior address needs one, it will be allocated the last, hence the oldest, exterior address on the available list.

All NAT configurations are *rule-based*. This means that traffic passed through NAT from either the public or the private network is compared to the rules and mappings configured in the Netopia R310 in a particular order. The first rule that applies to the traffic being initiated is used.

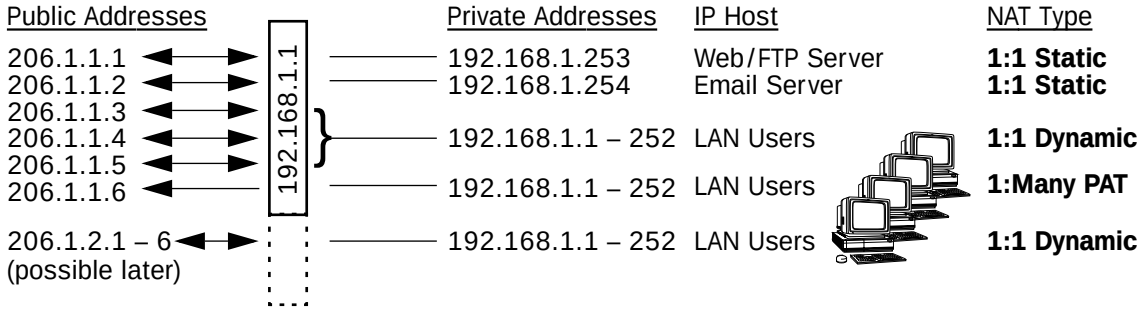
For example, if a connection is initiated from the public network and is destined for a public IP address configured on the Netopia R310, the following comparisons are made in this order.

- The Netopia R310 first checks its internal NAT cache to see if the data is part of a previously initiated connection, if not…
- The Netopia R310 checks the configured Server Lists to see if this traffic is intended to be forwarded to an internal host based on the type of service.
- The Netopia R310 then checks to see if there is a Static, Dynamic, or PAT mapping for the public IP address that the connection is being initiated to.
- The Netopia R310 answers the request itself if the data is destined for the Netopia's WAN interface IP address. Otherwise the data is discarded.

Complex maps

Map Lists and Server Lists are completely independent of each other. A Connection Profile can use one or the other or both.

MultiNAT allows complex mapping and requires seomwhat complex configuration. Multiple mapped interior subnets are supported, and the rules for mapping each of the subnets may be different. The figure below illustrates a possible multiNAT configuration.



In order to support this type of mapping, you define two address ranges. First, you define a public range which contains the first and last public address to be used and the way in which these addresses should be used (PAT, static, or dynamic). You then configure an address map which defines the private IP address or addresses to be used and which public range they should be mapped to. You add the address map to the list of address maps which are configured, creating a Map List. The mappings in the Map List are order-dependent and are compared in order from the top of the list to the bottom. If a particular resource is not available, subordinate mappings can be defined that will redirect traffic.

Additional Features

- Multiple public addresses, none of which have to be the same as the Connection Profile WAN IP address. Any public addresses not associated with the Connection Profile WAN IP address must have a static route pointing to it from a router on the public network if public users are expected to be able to access the NATed machines or services.
- Default PAT to a DHCP- or PPP-assigned address.
- 1:1 Dynamically Assigned NAT Mapping. This allows internal addresses to be temporarily assigned a public IP address to use for NAT. When the private host is finished communicating, the public IP address is made available for use by other internal hosts again.
- 1-to-1 static NAT mapping.

  An internal private address is permanently mapped to an external address. TCP and UDP port addresses are not altered.
- Multiple Many-to-1 PAT mappings on a single interface.

  PAT addresses may be assigned to specific private address subnets; not all internal machines need to be included on a PAT mapping list.
- Coexistent mapped and unmapped traffic on a public interface.

  If the router's IP address is not included in a NAT list, it will be invisible to the external network.
- Mapped services (exports) may use multiple public addresses.
- NAT maps per WAN interface, similar to the filter rules.

Supported traffic

MultiNat supports the following IP protocols:

- PAT: TCP/UDP traffic which does not carry source or destination IP addresses or ports in the data stream (i.e., HTTP, telnet, 'r' commands, tftp, NFS, NTP, SMTP, NNTP, etc.).
- Static NAT: All IP protocol traffic which does not carry or otherwise rely on the source or destination IP addresses in the data stream.
- Dynamic NAT: All IP protocol traffic which does not carry or otherwise rely on the source or destination IP addresses in the data stream.

MultiNAT Configuration

You configure the MultiNAT features through the console menu:

- For a simple 1-to-many NAT configuration (classic NAT), use the Basic configuration – Easy Setup Profile, described below.
- For the more advanced features, such as Server Lists and Dynamic NAT, follow the instructions in "IP setup" on page 9-7.

Basic configuration – Easy Setup Profile

The screen below is an example. Depending on the type of router you are using, fields displayed in this screen may vary.

```
                Connection Profile 1: Easy Setup Profile


        Number to Dial:                  2125551212

        Address Translation Enabled:     Yes
        IP Addressing...                 Unnumbered

        Local WAN IP Address:            206.1.1.6
        Local WAN IP Mask:               0.0.0.0
        Remote IP Address:               127.0.0.2
        Remote IP Mask:                  255.255.255.255

        PPP Authentication...            PAP
        Send User Name:                  tony
        Send Password:                   *****


        PREVIOUS SCREEN                  NEXT SCREEN

Enter the directory number for the remote network connection.
Enter basic information about your WAN connection with this screen.
```

The **Local WAN IP Address** is used to configure a NAT public address range consisting of the Local WAN IP Address and all its ports. The public address map list is named *Easy-PAT List* and the port map list is named *Easy-Servers*.

When you exit this screen the two map lists, Easy-PAT List and Easy-Servers, are created by default and NAT configuration becomes effective.This will map all your private addresses (0.0.0.0 through 255.255.255.255) to your public address. These map lists are bound to the Easy Setup Profile. See "Binding Map Lists and Server Lists" on page 9-20.

This is all you need to do if you want to continue to use a single PAT, or 1-to-many, NAT configuration.

Advanced configuration – Server Lists and Dynamic NAT

You use the advanced NAT feature sets by first defining a series of mapping rules and then grouping them into a *list*. There are two kinds of lists -- *Map Lists*, made up of Dynamic, PAT and Static mapping rules, and *Server Lists*, a list of internal services to be presented to the external world. Creating these lists is a four-step process:

1. **Define the public range** of addresses that external computers should use to get to the NAT internal machines. These are the addresses that someone on the Internet would see.
2. **Create a List name** that will act as a rule or server holder.
3. **Create a *map* or rule** that specifies the internal range of NATed addresses and the external range they are to be associated with.
4. **Associate the Map or Server List to your WAN interface** via a Connection Profile or the Default Profile.

The three NAT features all operate completely independently of each other, although they can be used simultaneously on the same Connection Profile.

You can configure a simple 1-to-many PAT (often referred to simply as NAT) mapping using Easy Setup. More complex setups require configuration using the **Network Address Translation** item on the IP Setup screen.

An example MultiNAT configuration at the end of this chapter describes some applications for these features. See "MultiNAT Configuration Example" on page 9-24.

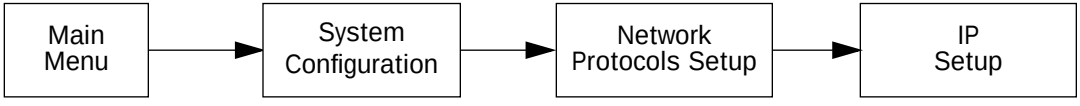
In order to configure the router to make servers on your LAN visible to the Internet, you use advanced features in the System Configuration screens, described in "IP setup," below.

Note: There is no implicit binding between the WAN IP interface address and NAT, so you cannot disallow configuration of NAT simply because the interface is numbered or disallow configuration of the addressing type (numbered or unnumbered) simply because NAT is enabled.

If the router has a numbered interface, then it is addressable by the IP address. Also, MultiNAT adds the option of true unnumbered NAT. Traffic delivered to the router on an unnumbered interface which cannot be processed by NAT is dropped.

IP setup

To access the NAT configuration screens, from the Main Menu navigate to IP Setup:



```
                                IP Setup

        Ethernet IP Address:              192.168.1.1
        Ethernet Subnet Mask:             255.255.255.0
        Define Additional Subnets...

        Default IP Gateway:               0.0.0.0

        Primary Domain Name Server:       0.0.0.0

        Domain Name:                      isp.com

        Receive RIP:                      Both
        Transmit RIP:                     Off
        Static Routes...

        IP Address Serving Setup
        Network Address Translation (NAT)...
        Filter Sets...

Enter an IP address in decimal and dot form (xxx.xxx.xxx.xxx).
Set up the basic IP attributes of your Netopia in this screen.
```

Select **Network Address Translation (NAT)** and press Return.

The Network Address Translation screen appears.

```
                        Network Address Translation

                    Add Public Range...
                    Show/Change Public Range...
                    Delete Public Range...

                    Add Map List...
                    Show/Change Map List...
                    Delete Map List...

                    Add Server List...
                    Show/Change Server List...
                    Delete Server List...

                    NAT Associations...




Return/Enter to configure IP Address redirection.
```

Public Range. defines an external address range and indicates what type of mapping to apply when using this range. The types of mapping available are *dynamic*, *static* and *pat*.

Map Lists. define collections of mapping rules. A rule maps interior range addresses to exterior range addresses by the mapping techniques defined in the map list.

Server Lists. bind internal IP addresses and ports to external IP addresses and ports so that connections initiated from the outside can access an interior server.

NAT rules

The following rules apply to assigning NAT ranges and server lists:

- Static public address ranges must not overlap other static, PAT, public addresses or the public address assigned to the router's WAN interface.
- A PAT public address must not overlap any static address ranges. It may be the same as another PAT address or server list address, but the port range must not overlap.

You configure the ranges of exterior addresses by first adding public ranges.

Select **Add Public Range** and press Return.

The Add NAT Public Range screen appears.

```
                    Add NAT Public Range

Range Name:                         my_first_range
Type...                             pat
Public Address:                     206.1.1.6

First Public Port:                  49152
Last Public Port:                   65535


ADD NAT PUBLIC RANGE                CANCEL
```

- Select **Range Name** and give a descriptive name to this range.
- Select **Type** and from the pop-up menu, assign its type. Options are static, dynamic, or pat (the default).
  - If you choose *pat* as the range type, select **Public Address** and enter the exterior IP address in the range you want to assign. Select **First** and **Last Public Port** and enter the first and last exterior ports in the range. These are the ports that will be used for traffic initiated from the private LAN to the outside world.

    Note: For PAT Map lists and Server lists, if you use the Public Address 0.0.0.0, the list will acquire its public IP address from the WAN IP address specified by your WAN IP configuration in the Connection Profile. If that is a static IP address, then the PAT map list and Server lists will acquire that address. If it is a negotiated IP address, such as may be assigned via DHCP or PPP, the PAT map list and Server lists will acquire that address each time it is negotiated.
  - If you choose *dynamic* as the range type, a new menu item, **First Public Address**, becomes visible. Select **First Public Address** and enter the first exterior IP address in the range you want to assign. Select **Last Public Address** and enter an IP address at the end of the range.

- If you choose *static* as the range type, a new menu item, **First Public Address**, becomes visible. Select **First Public Address** and enter the first exterior IP address in the range you want to assign. Select **Last Public Address** and enter an IP address at the end of the range.

- Select **ADD NAT PUBLIC RANGE** and press Return. The range will be added to your list and you will be returned to the Network Address Translation screen.

Once the public ranges have been assigned, the next step is to bind interior addresses to them. Because these bindings occur in ordered lists, called *map lists*, you must first define the list, then add mappings to it.

From the Network Address Translation screen select **Add Map List** and press Return.

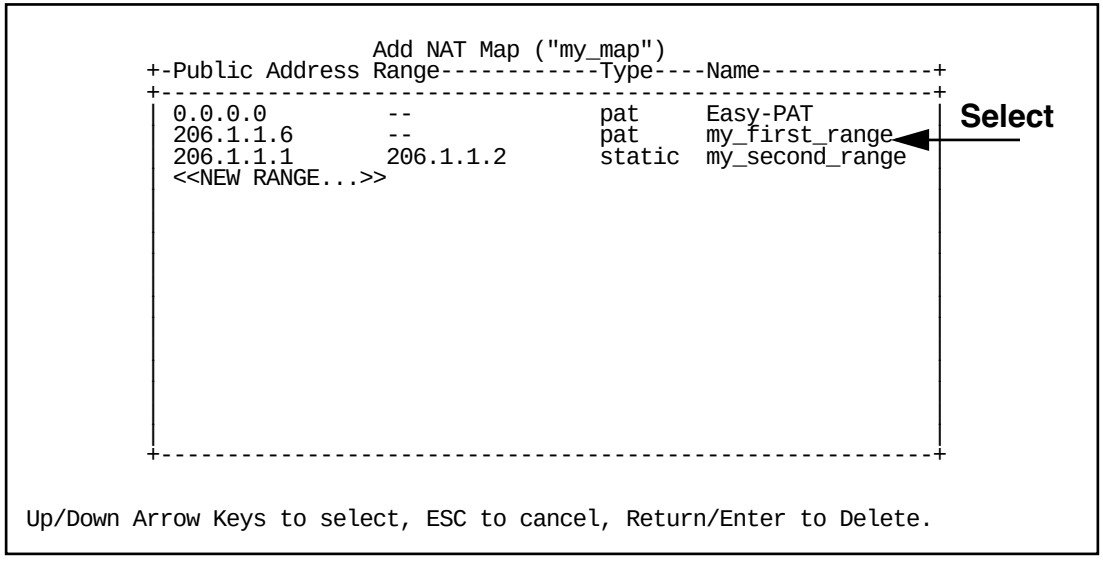
The Add NAT Map List screen appears.

```
                          Add NAT Map List

        Map List Name:                    my_map

        Add Map...
```

- Select **Map List Name** and enter a descriptive name for this map list. A new menu item **Add Map** appears.
- Select **Add Map** and press Return. The Add NAT Map screen appears.

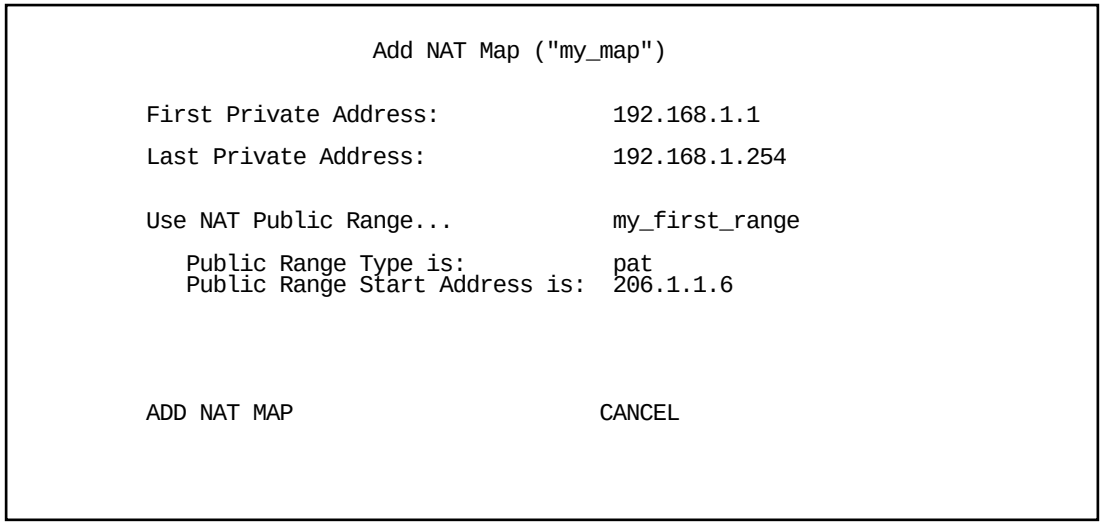
```
                    Add NAT Map ("my_map")

        First Private Address:            192.168.1.1
        Last Private Address:             192.168.1.254

        Use NAT Public Range...



        ADD NAT MAP                       CANCEL
```

- Select **First** and **Last Private Address** and enter the first and last interior IP addresses you want to assign to this mapping.
- Select **Use NAT Public Range** and press Return. A screen appears displaying the public ranges you have defined.



- From the list of public ranges you defined, select the one that you want to map to the interior range for this mapping and press Return.

  If none of your preconfigured ranges are suitable for this mapping, you can select **<<NEW RANGE>>** and create a new range. If you choose **<<NEW RANGE>>**, the Add NAT Public Range screen displays and you can create a new public range to be used by this map. See "Add NAT Public Range" on page 9-9.
- The Add NAT Map screen now displays the range you have assigned.



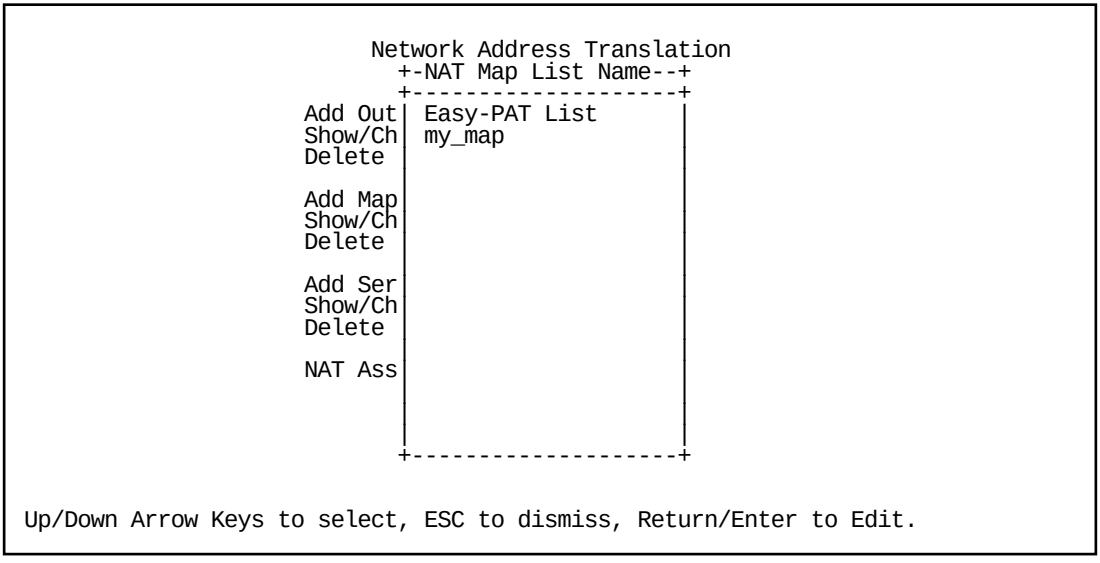
- Select **ADD NAT MAP** and press Return. Your mapping is added to your map list.

Modifying map lists

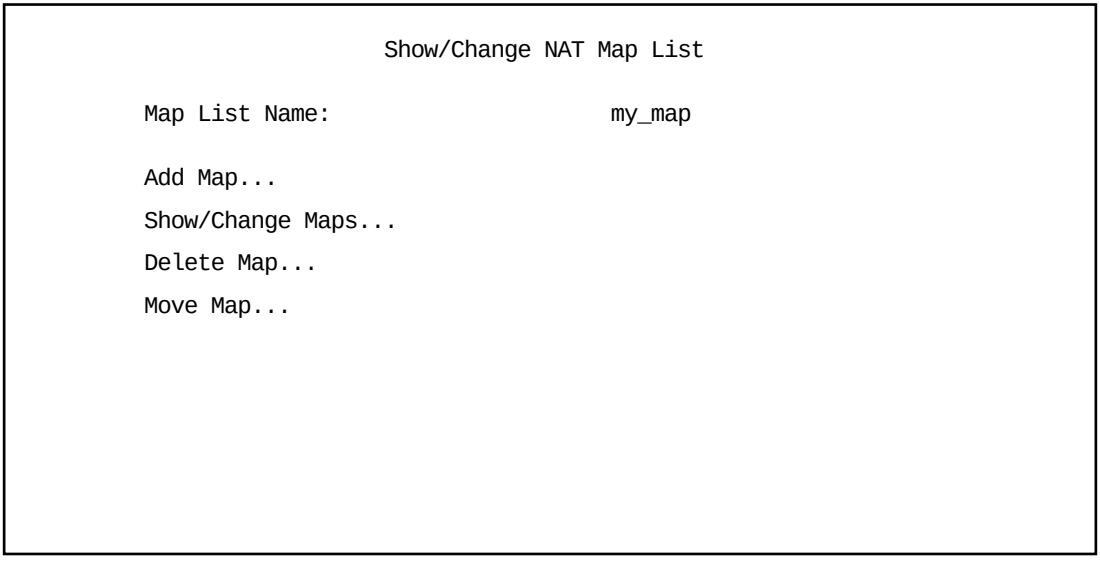
You can make changes to an existing map list after you have created it. Since there may be more than one map list you must select which one you are modifying.

From the Network Address Translation screen select **Show/Change Map List** and press Return.

- Select the map list you want to modify from the popup menu.

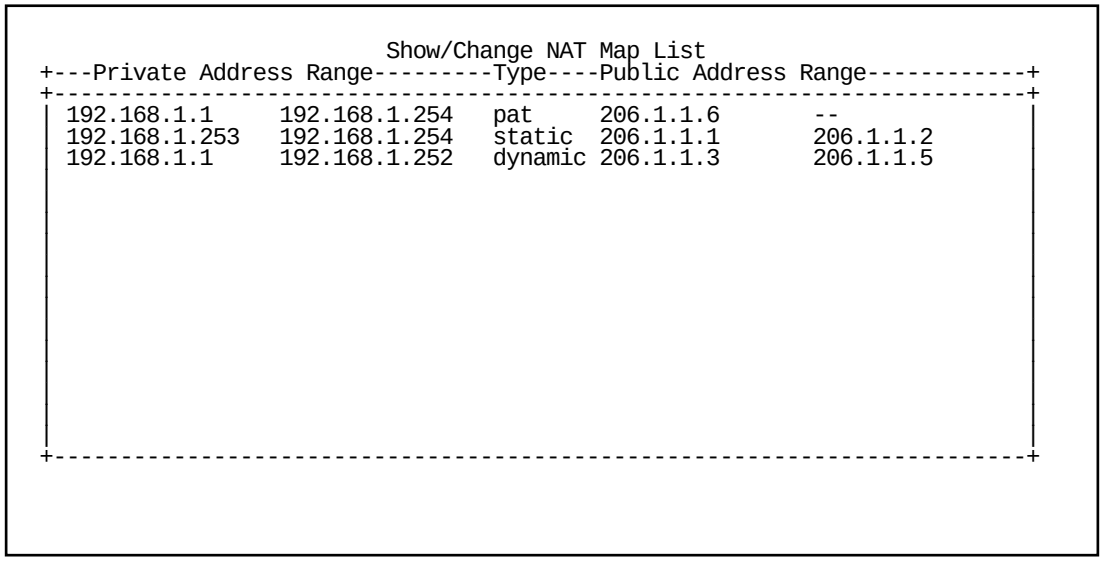


The Show/Change NAT Map List screen appears.



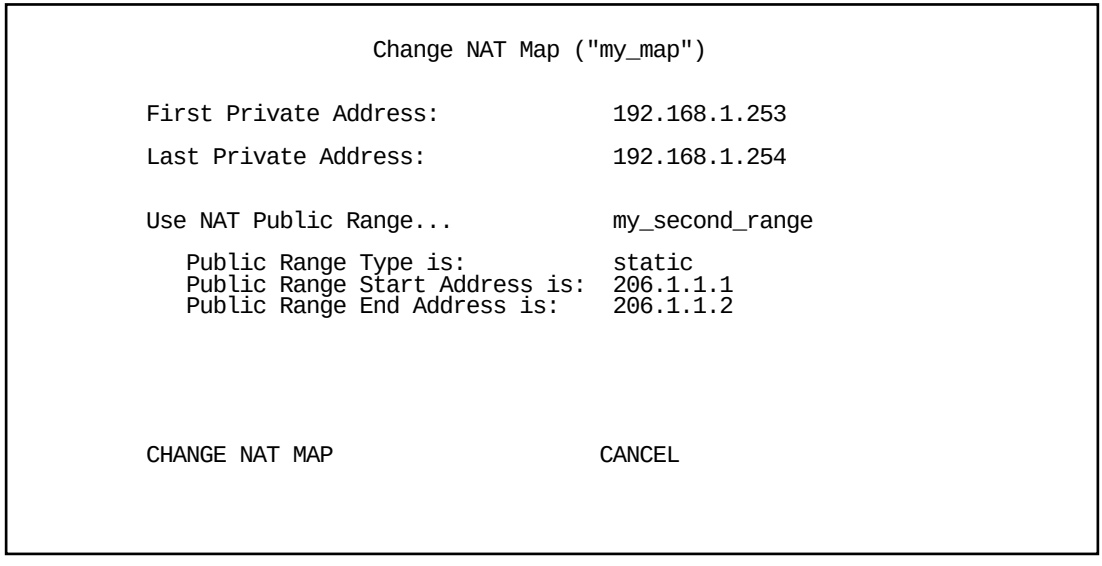
- **Add Map** allows you to add a new map to the map list.
- **Show / Change Maps** allows you to modify the individual maps within the list.
- **Delete Map** allows you to delete a map from the list.
- **Move Map** allows you to change the priority order in which the map is evaluated within the list. See "Moving maps" on page 9-14.

Selecting **Show / Change Maps**, **Delete Map**, or **Move Map** displays the same pop-up menu.



Scroll to the map you want to modify using the arrow keys and press Return.

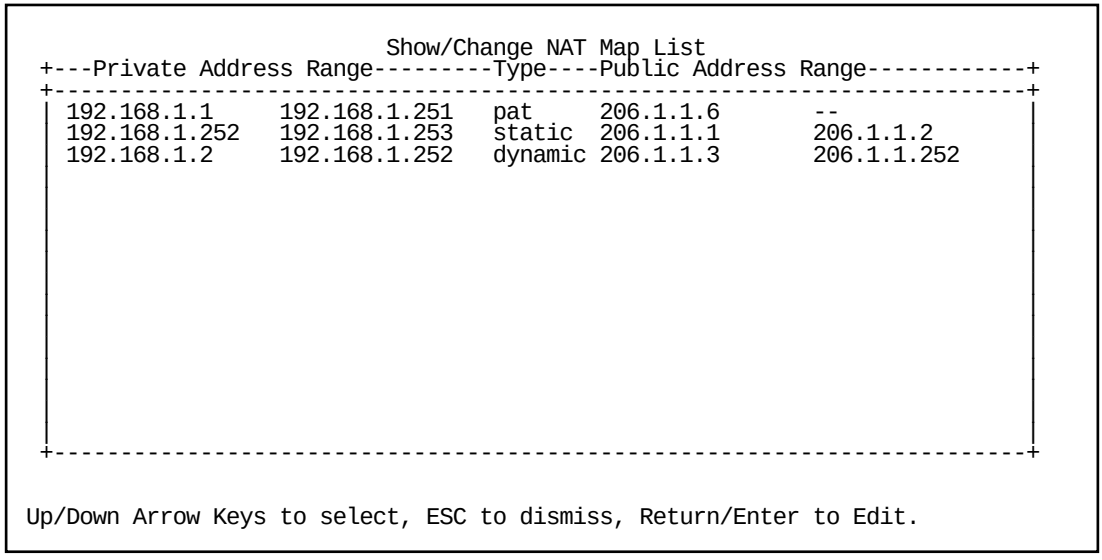
The Change NAT Map screen appears.



Make any modifications you need and then select **CHANGE NAT MAP** and press Return. Your changes will become effective and you will be returned to the Show/Change NAT Map List screen.

Moving maps

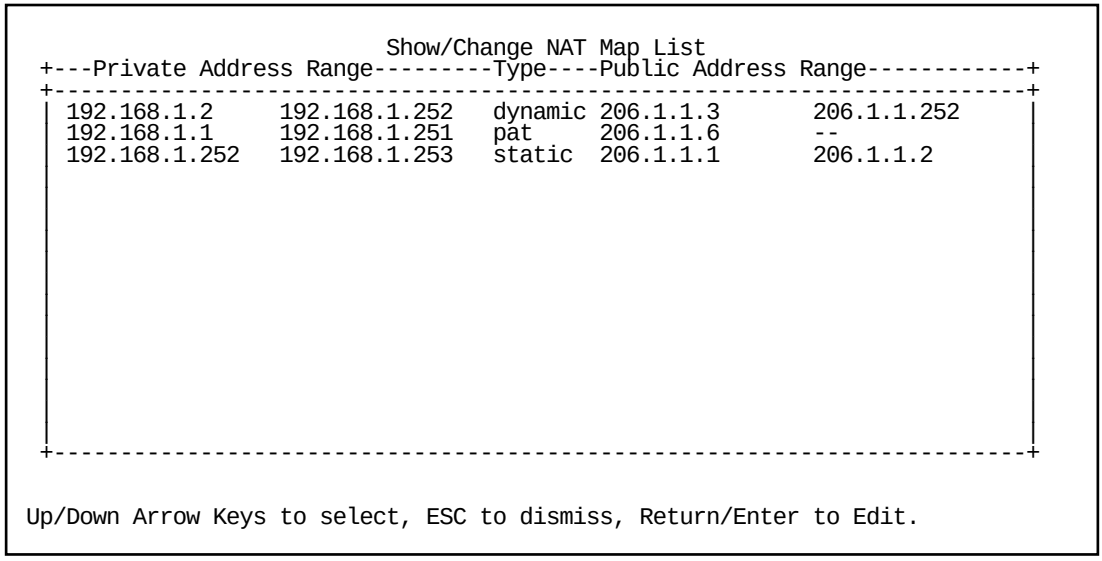
The Move Maps screen permits reordering the priority of maps in a map list. Since the maps are read from top to bottom, those at the top have the highest priority, those at the bottom have the lowest. If you used Easy Setup for your initial configuration, and added subsequent maps and server lists, you may need to reorder their priority since new maps are added to the top of the list.



In the example screen above, you may want to reorder the priority of the maps such that the dynamic map applies first and any additional traffic is routed via PAT or static.

All operations are done from a single pop-up menu.

- In the Show/Change Map List screen, select **Move Map**. A selection mode pop-up menu appears. In this mode you scroll to the map you want to move and press **Return** to select it for moving.
- After pressing **Return** you are in Move mode. Arrow keys move the selected map up or down. When you press **Return** again the map is put in the new location permanently and the pop-up menu is dismissed.



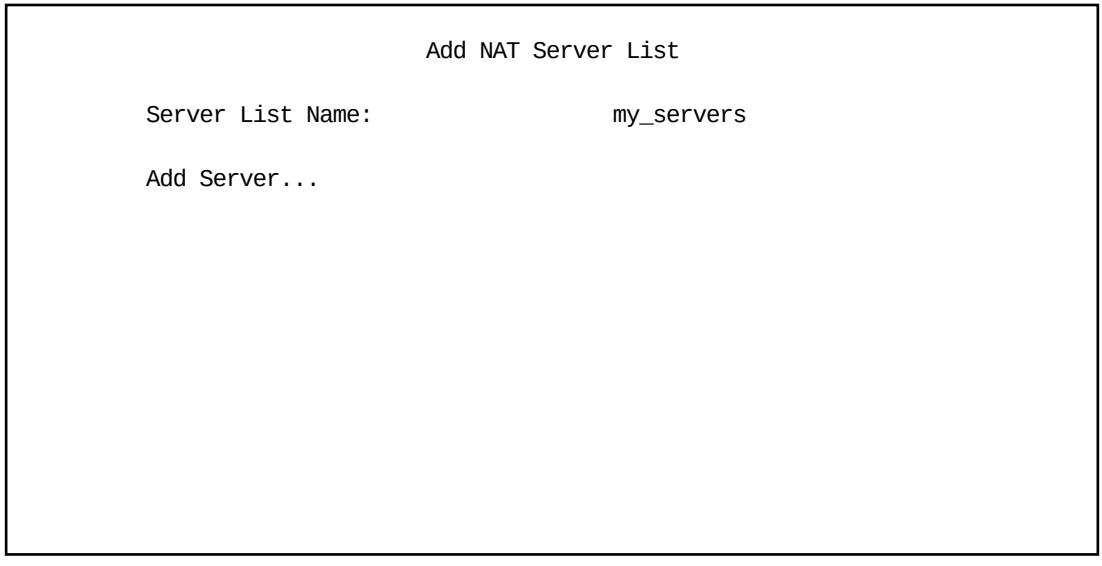
- You can press **Escape** at any time in the pop-up menu to abort the move and restore the map list to its original ordering.

Adding Server Lists

Server lists, also known as Exports, are handled similarly to map lists. If you want to make a particular server's port accessible (and it isn't accessible through other means, such as a static mapping), you must create a Server List.

Select **Add Server List** from the Network Address Translation screen.

The Add NAT Server List screen appears.



- Select **Server List Name** and type in a descriptive name. A new menu item, **Add Server**, appears.
- Select **Add Server** and press Return. The Add NAT Server screen appears.

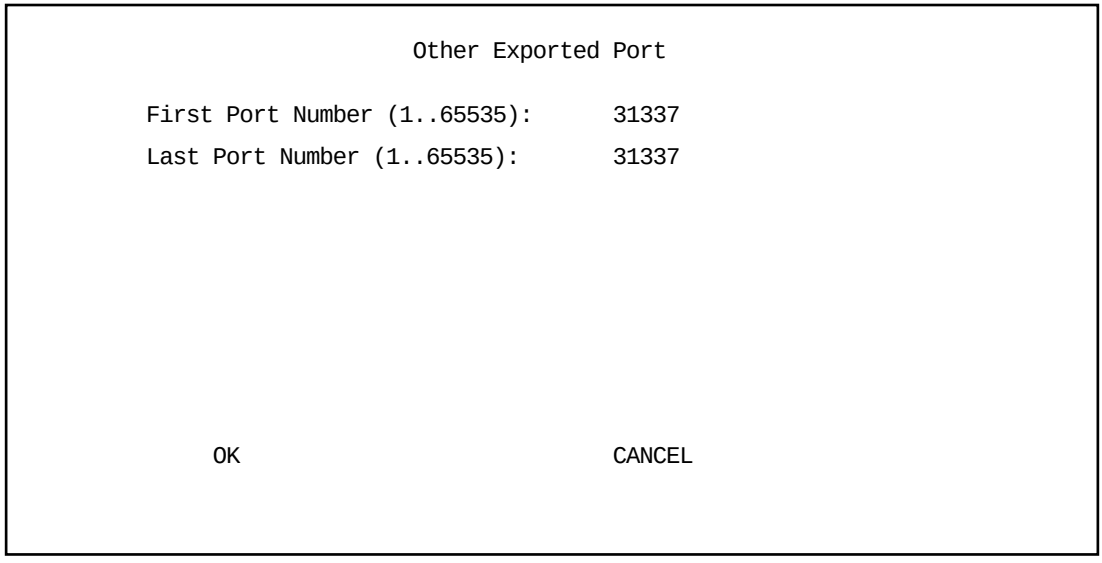
```
                    Add NAT Server ("my_servers")

        Service...
        Server Private IP Address:          192.168.1.45
        Public IP Address:                  206.1.1.1









        ADD NAT SERVER                      CANCEL
```

- Select **Service** and press Return. A pop-up menu appears listing a selection of commonly exported services.

```
                    Add NAT Server ("my_servers")
                                  +-Type------Port(s)-------+
                                  +-------------------------+
        Service...                | ftp       21            |
                                  | telnet    23            |
        Server Private IP Address:| smtp      25            |
                                  | tftp      69            |
        Public IP Address:        | gopher    70            |
                                  | finger    79            |
                                  | www-http  80            |
                                  | pop2      109           |
                                  | pop3      110           |
                                  | snmp      161 - 162     |
                                  | timbuktu  407           |
                                  | pptp      1723          |
                                  | irc       6665 - 6669   |
                                  | Other...                |
                                  +-------------------------+
        ADD NAT SERVER              CANCEL
```

- Choose the service you want to export and press Return.

  You can choose a preconfigured service from the list, or define your own by selecting **Other**. If you select **Other**, a screen is displayed that allows you to enter the port number range for your customized service.



- Enter the **First** and **Last Port Number** between ports 1 and 65535. Select **OK** and press Return. You will be returned to the Add NAT Server screen.

- Enter the **Server Private IP Address** of the server whose service you are exporting.

  Since MultiNAT permits the mapping of multiple private IP addresses to multiple public IP addresses, your ISP or corporate site's router must be configured such that it knows that your multiple public addresses are accessible via your router.

  If you want to use static mappings to map internal servers to public addresses, your ISP or corporate site's router must also be configured for static routes to these public addresses on the Netopia R310.

- Enter the **Public IP Address** to which you are exporting the service.

  Note: For PAT Map lists and Server lists, if you use the Public Address 0.0.0.0, the list will acquire its public IP address from the WAN IP address specified by your WAN IP configuration in the Connection Profile. If that is a static IP address, then the PAT map list and Server lists will acquire that address. If it is a negotiated IP address, such as may be assigned via DHCP or PPP, the PAT map list and Server lists will acquire that address each time it is negotiated.

- Select **ADD NAT SERVER** and press Return. The server will be added to your server list and you will be returned to the Add NAT Server List screen.

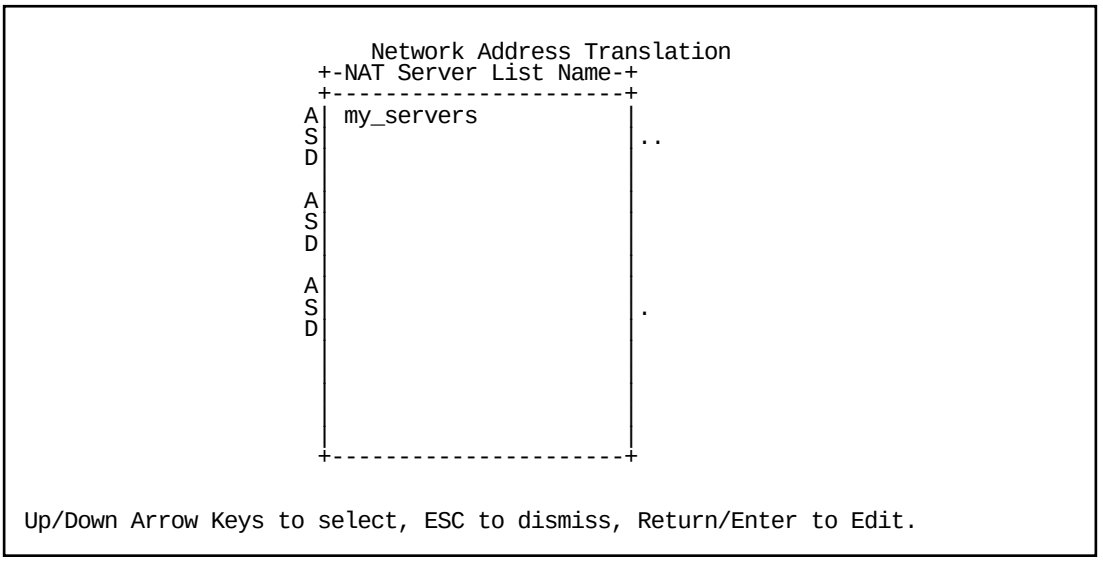
Note: To use **CUSeeMe** (or other services that listen on specific ports) through the Netopia R310, you must export the ports 7648 *and* 7649. In MultiNat, you may use a port range export. Without the export, CUSeeMe will fail to work. This is true unless a static mapping is in place for the host using CUSeeMe. In that case no Server List entry is necessary.

Modifying server lists

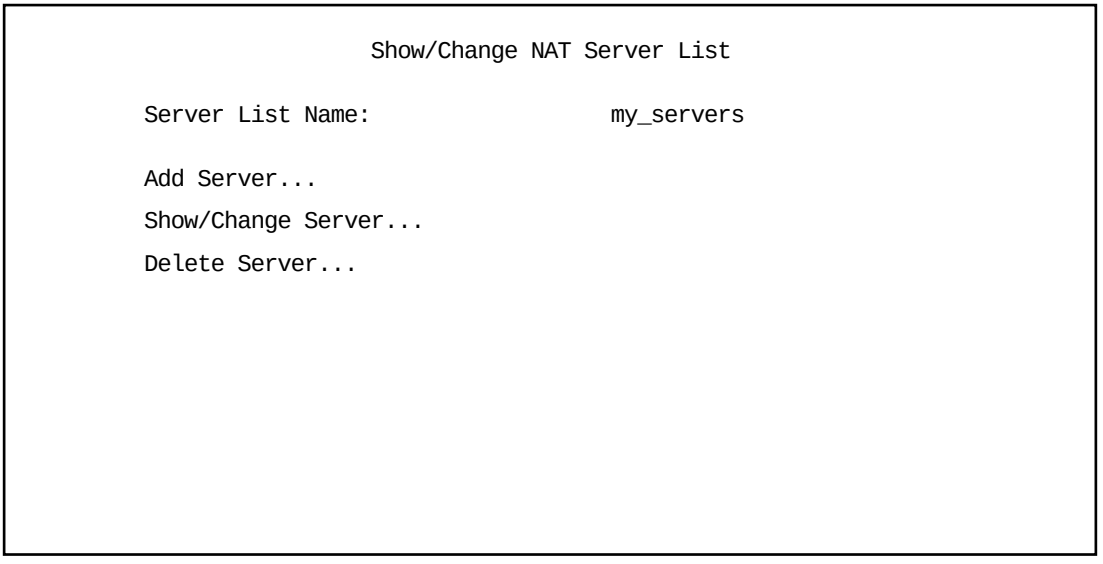
Once a server list exists, you can select it for modification or deletion.

- Select **Show / Change Server List** from the Network Address Translation screen.

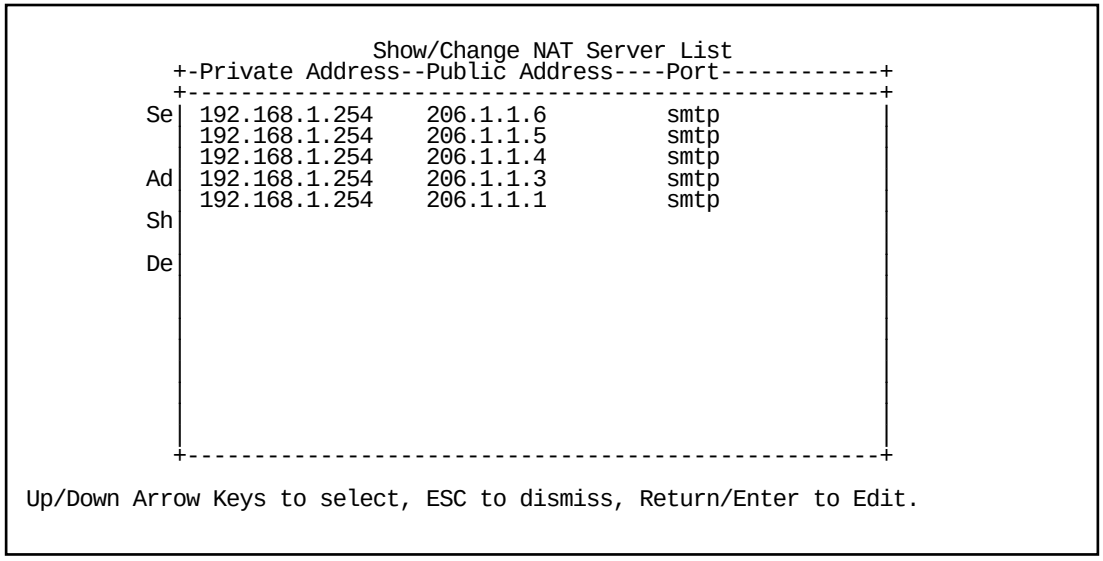
- Select the Server List Name you want to modify from the pop-up menu and press Return.



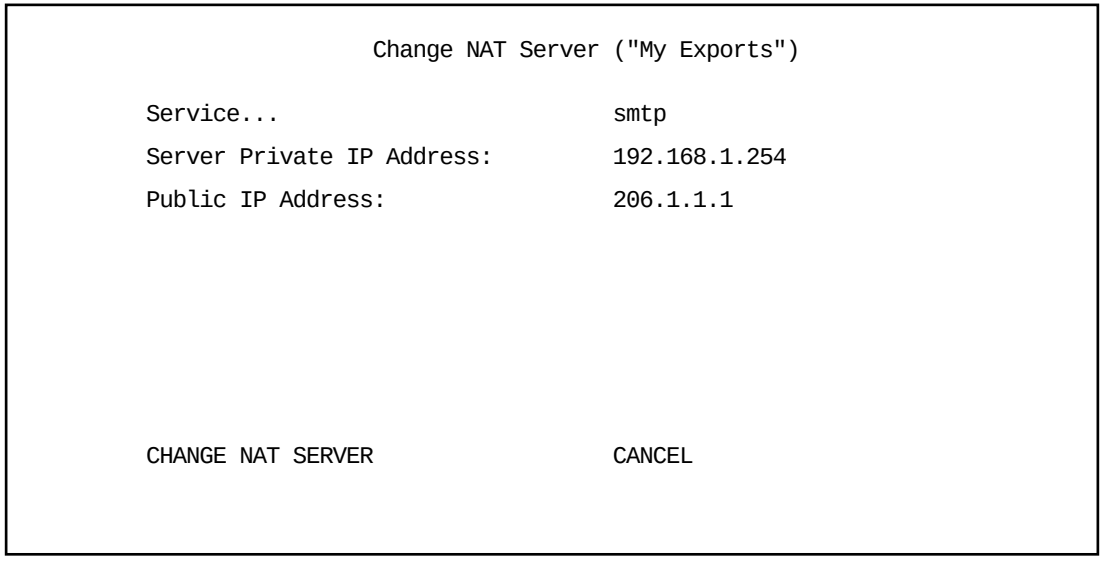
The Show/Change NAT Server List screen appears.



- Selecting **Show/Change Server** or **Delete Server** displays the same pop-up menu.



Select any server from the list and press **Return**. The Change NAT Server screen appears.



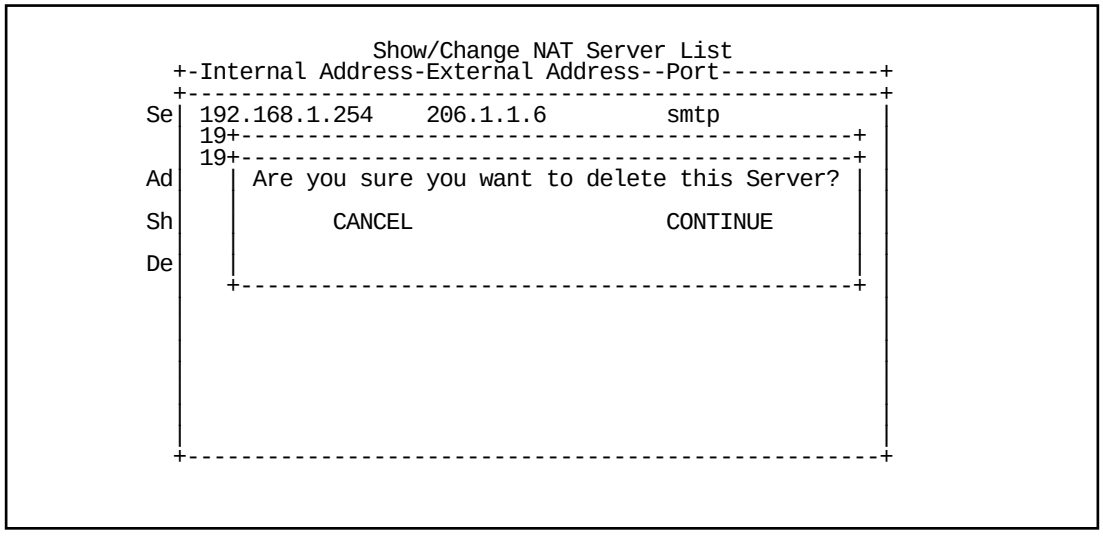
You can make changes to the server's service and port or internal or external address.

Select **CHANGE NAT SERVER** and press Return. Your changes take effect and you are returned to the Show/Change NAT Server List screen.

Deleting a server

To delete a server from the list, select **Delete Server** from the Show/Change NAT Server List menu and press Return.

A pop-up menu lists your configured servers. Select the one you want to delete and press Return. A dialog box asks you to confirm your choice.



Choose **CONTINUE** and press Return. The server is deleted from the list.

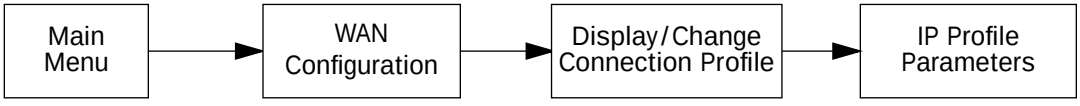
Binding Map Lists and Server Lists

Once you have created your map lists and server lists, you must bind them to a profile, either a Connection Profile or the Default Profile. You do this in one of the following screens:

- the IP profile parameters screen (see below) of the Connection Profile configuration menu
- the NAT Associations screen (see page 9-22)
- the Binding Map Lists and Server Lists screen (see page 9-20)

IP profile parameters

To bind a map list to a Connection Profile, from the Main Menu go to the WAN Configuration screen then the Display/Change Connection Profile screen. From the pop-up menu list of your Connection Profiles, choose the one you want to bind your map list to. Select **IP Profile Parameters** and press Return.



The IP Profile Parameters screen appears.

```
                          IP Profile Parameters

        Address Translation Enabled:       Yes
        IP Addressing...                   Unnumbered

        NAT Map List...                    Easy-PAT List
        NAT Server List...                 Easy-Servers

        Local WAN IP Address:              206.1.1.6

        Remote IP Address:                 127.0.0.2
        Remote IP Mask:                    255.255.255.255

        Filter Set...                      NetBIOS Filter
        Remove Filter Set

        Receive RIP:                       Both


Return/Enter to select <among/between> ...
Configure IP requirements for a remote network connection here.
```

- Select **NAT Map List** and press Return. A pop-up menu displays a list of your defined map lists.

```
                          IP Profile Parameters
                     +--NAT Map List Name---+
                     +----------------------+
        Address Trans| Easy-PAT             |s
        IP Addressing| my_map               |mbered
                     | <<None>>             |
        NAT Map List.|                      |sy PAT
        NAT Server Li|                      |
                     |                      |
        Local WAN IP |                      |
                     |                      |
        Remote IP Add|                      |7.0.0.2
        Remote IP Mas|                      |5.255.255.255
                     |                      |
        Filter Set...|                      |tBIOS Filter
        Remove Filter|                      |
                     |                      |
        Receive RIP: |                      |th
                     |                      |
                     +----------------------+


Up/Down Arrow Keys to select, ESC to dismiss, Return/Enter to Edit.
```

- Select the map list you want to bind to this Connection Profile and press Return. The map list you selected will now be bound to this Connection Profile.
- Select **NAT Server List** and press Return. A pop-up menu displays a list of your defined server lists.

```
                        IP Profile Parameters
                    +-NAT Server List Name-+
                    +----------------------+
          Address Trans| Easy-Servers        |s
          IP Addressing| my_servers          |mbered
                       | <<None>>
          NAT Map List.|                     |sy PAT
          NAT Server Li|                     |

          Local WAN IP |                     |0.0.0
          Local WAN IP |                     |0.0.0
          Remote IP Add|                     |7.0.0.2
          Remote IP Mas|                     |5.255.255.255

          Filter Set...|                     |tBIOS Filter
          Remove Filter|                     |

          Receive RIP: |                     |th
                       |                     |
                    +----------------------+


Up/Down Arrow Keys to select, ESC to dismiss, Return/Enter to Edit.
```

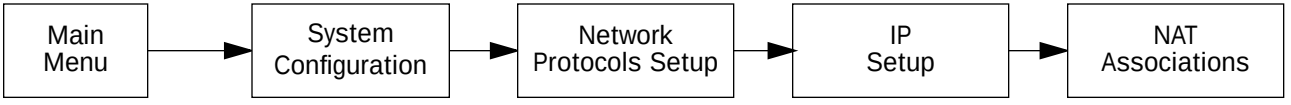
- Select the server list you want to bind to this Connection Profile and press Return. The server list you selected will now be bound to this Connection Profile.

Note: There is no interdependency between NAT and IP Addressing. Also, the Local WAN IP Address and Mask fields' visibility are dependent only on the IP Addressing type.

NAT Associations

Configuration of map and server lists alone is not sufficient to enable NAT for a WAN connection because map and server lists must be linked to a profile that controls the WAN interface. This can be a Connection Profile, a WAN Ethernet interface, a default profile, or a default answer profile. Once you have configured your map and server lists, you may want to reassign them to different interface-controlling profiles, for example, Connection Profiles. To permit easy access to this IP Setup functionality, you can use the NAT Associations screen.

You access the NAT Associations screen from the Network Address Translation screen.



Select **NAT Associations** and press Return. The NAT Associations screen appears.

```
                              NAT Associations

    Profile/Interface Name-------------Nat?-Map List Name-----Server List Name
    Default Answer Profile              On   my_first_map      my_servers
    Easy Setup Profile                  On   Easy-PAT          my_servers
    Profile 01                          On   my_second_map     my_servers
    Profile 02                          On   my_first_map      my_server_list
    Profile 03                          On   <<None>>          <<None>>
```

- You can toggle **NAT? On** or **Off** for each Profile/Interface name. You do this by navigating to the **NAT?** field associated with each profile using the arrow keys. Toggle NAT on or off by using the Tab key.
- You can reassign any of your map lists or server lists to any of the Profile/Interfaces. You do this by navigating to the **Map List Name** or **Server List Name** field associated with each profile using the arrow keys. Select the item by pressing Return to display a pop-up menu of all of your configured lists.

```
                              NAT Associations
                                    +NAT Map List Name-+
    Profile/Interface Name-------------Nat+------------------+Server List Name
    Easy Setup Profile                  On | Easy-PAT List    |my_servers
    Profile 01                          On | my_first_map     |my_servers
    Profile 02                          On | my_second_map    |my_server_list
    Profile 03                          On | my_map           |<<None>>
    Profile 04                          On | <<None>>         |<<None>>
                                           |                  |
                                           |                  |
                                           |                  |
                                           |                  |
                                           |                  |
                                           |                  |
                                           |                  |
                                           |                  |
    Default Answer Profile              On +------------------+my_servers

Up/Down Arrow Keys to select, ESC to dismiss, Return/Enter to Edit.
```

- Select the list name you want to assign and press Return again. Your selection will then be associated with the corresponding profile or interface.

MultiNAT Configuration Example

To help you understand a typical MultiNAT configuration, this section describes an example of the type of configuration you may want to implement on your site. The values shown are for example purposes only. *Make your own appropriate substitutions.*

A typical SDSL service from an ISP might include five user addresses. Without PAT, you might be able to attach only five IP hosts. Using simple 1-to-many PAT you can connect more than five devices, but use only one of your addresses. Using multiNAT you can make full use of the address range. The example assumes the following range of addresses offered by a typical ISP:

Local WAN IP address:	206.1.1.6
Local WAN subnet mask:	255.255.255.248
Remote IP address:	206.1.1.254
Default gateway:	206.1.1.254

Public IP addresses assigned by the ISP are 206.1.1.1 through 206.1.1.6 (255.255.255.248 subnet mask).

Your internal devices have IP addresses of 192.168.1.1 through 192.168.1.254 (255.255.255.0 subnet mask).

Netopia R310's address is:	192.168.1.1
Web server's address is:	192.168.1.253
Mail server's address is:	192.168.1.254
FTP server's address is:	192.168.1.253

In this example you will statically map the first five public IP addresses (206.1.1.1 - 206.1.1.5) to the first five corresponding private IP addresses (192.168.1.1 - 192.168.1.5). You will use these 1-to-1 mapped addresses to give your servers "real" addresses. You will then map 206.1.1.6 to the remaining private IP addresses (192.168.1.6 - 192.168.1.254) using PAT.

The configuration process is as follows:

From the Main Menu go to the Easy Setup and then the Connection Profile screen.

Enter your ISP-supplied values as shown below.

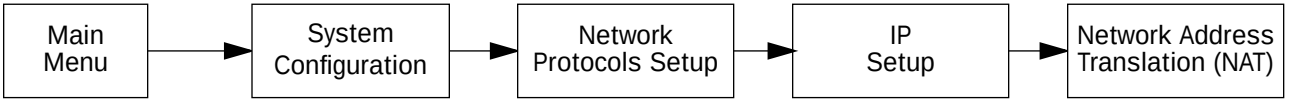
```
                Connection Profile 1: Easy Setup Profile

        Connection Profile Name:          Easy Setup Profile


        Address Translation Enabled:      Yes
        IP Addressing...                  Numbered

        Local WAN IP Address:             206.1.1.6
        Local WAN IP Mask:                255.255.255.248









        PREVIOUS SCREEN                   NEXT SCREEN

Enter a subnet mask in decimal and dot form (xxx.xxx.xxx.xxx).
Enter basic information about your WAN connection with this screen.
```

Select **NEXT SCREEN** and press Return.

Your IP values are shown here.

```
                            IP Easy Setup


        Ethernet IP Address:              192.168.1.1
        Ethernet Subnet Mask:             255.255.255.0

        Domain Name:                      ISP.net
        Primary Domain Name Server:       173.166.101.1
        Secondary Domain Name Server:     173.166.102.1

        Default IP Gateway:               127.0.0.2
        IP Address Serving:               On

        Number of Client IP Addresses:    20
        1st Client Address:               192.168.1.2


        PREVIOUS SCREEN                   NEXT SCREEN

Set up the basic IP attributes of your Netopia in this screen.
```

Then navigate to the Network Address Translation (NAT) screen.



Select **Show / Change Public Range**, then **Easy-PAT Range**, and press Return. Enter the value your ISP assigned for your public address (206.1.1.6, in this example). Toggle **Type** to *pat*. Your public address is then mapped to the remaining private IP addresses using PAT. (If you were not using the Easy-PAT Range and Easy-PAT List that is created by default by using Easy Setup, you would have to *define* a public range and Map List. For the purpose of this example you can just *alter* this range and list.)

```
                    Change NAT Public Range

        Range Name:                     Easy-PAT Range
        Type...                         pat
        Public Address:                 206.1.1.6

        First Public Port:              49152
        Last Public Port:               65535



        CHANGE NAT PUBLIC RANGE         CANCEL
```

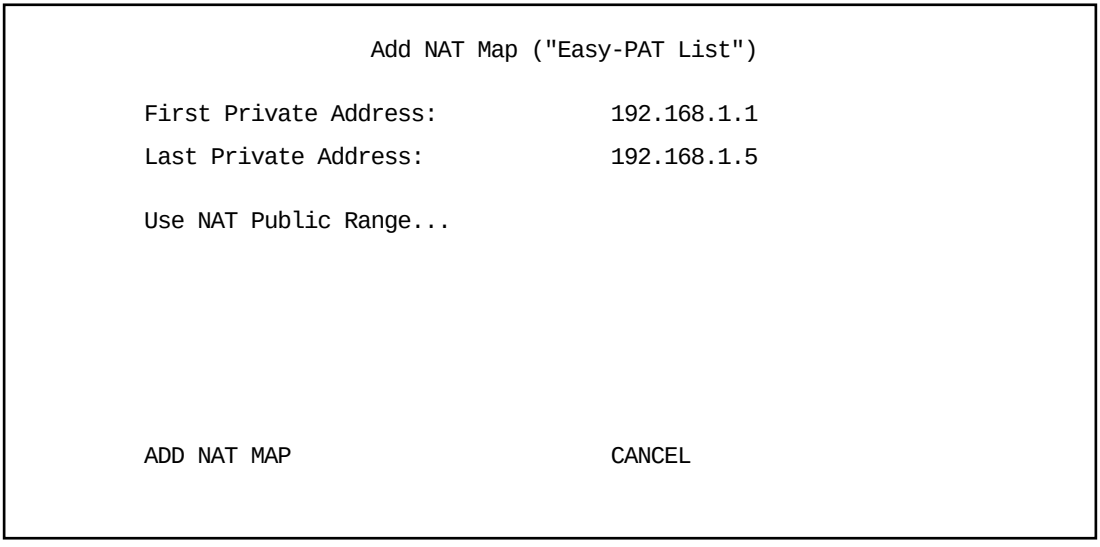
Select **CHANGE NAT PUBLIC RANGE** and press Return. This returns you to the Network Address Translation screen.

Select **Add Public Range** and press Return. Type a name for this static range, as shown below. Enter the first and last public addresses your ISP assigned in their respective fields as shown. The first five public IP addresses (206.1.1.1 - 206.1.1.5, in this example) are statically mapped to the first five corresponding private IP addresses (192.168.1.1 - 192.168.1.5).

```
                    Add NAT Public Range

        Range Name:                     Static Range
        Type...                         static
        First Public Address:           206.1.1.1
        Last Public Address:            206.1.1.5







        ADD NAT PUBLIC RANGE            CANCEL
Return/Enter to commit changes.
```

Select **ADD NAT PUBLIC RANGE** and press Return. You are returned to the **Network Address Translation** screen.

Next, select **Show / Change Map List** and choose **Easy-PAT List**. Select **Add Map**. The **Add NAT Map** screen appears. (Now the name *Easy-PAT List* is a misnomer since it has a static map included in its list.) Enter in 192.168.1.1 for the **First Private Address** and 192.168.1.5 for the **Last Private Address**.



Select **Use NAT Public Range** and from the pop-up menu choose **Static Range**. Select **ADD NAT MAP** and press Return.

This will statically map the first five public IP addresses to the first five corresponding private IP addresses and will map 206.1.1.6 to the remaining private IP addresses using PAT.

Notes on the example

The Easy-Map List and the Easy-PAT List are attached to any new Connection Profile by default. If you want to use this NAT configuration on a previously defined Connection Profile then you need to *bind* the Map List to the profile. You do this through either the NAT Associations screen or the profile's configuration screens.

The PAT part of this example setup will allow any user on the Netopia R310's LAN with an IP address in the range of 192.168.1.6 through 192.168.1.254 to *initiate* traffic flow to the outside world (for example, the Internet). No one on the Internet would be able to initiate a conversation with them.

The Static mapping part of this example will allow any of the machines in the range of addresses from 192.168.1.1 through 192.168.1.5 to communicate with the outside world as if they were at the addresses 206.1.1.1 through 206.1.1.5, respectively. It also allows any machine on the Internet to access any service (port) on any of these five machines.

You may decide this poses a security risk. You may decide that anyone can have complete access to your FTP server, but not to your router, and only limited access to the desired services (ports) on the Web and Mail servers.

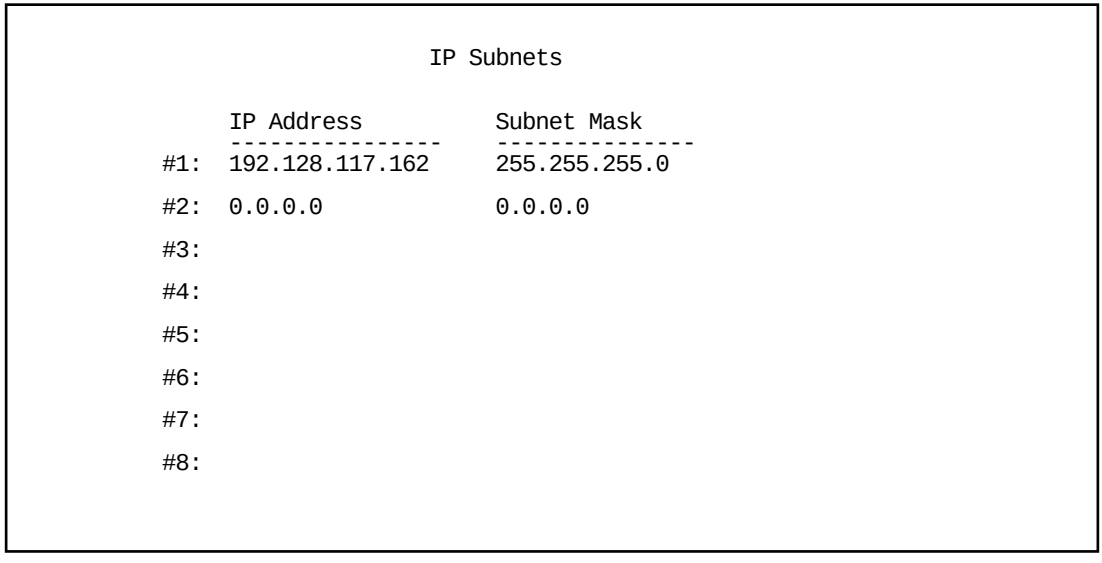
To make these changes, first limit the range of remapped addresses on the Static Map and then edit the default Server List called Easy-Servers.

- First, navigate to the **Show / Change Map List** screen, select **Easy-PAT List** and then **Show / Change Maps**. Choose the **Static Map** you created and change the **First Private Address** from 192.168.1.1 to 192.168.1.4. Now the router, Web, and Mail servers' IP addresses are no longer included in the range of static mappings and are therefore no longer accessible to the outside world. Users on the Internet will not be able to telnet, web, SNMP or ping to them. It is best also to navigate to the public range screen and change the **Static Range** to go from 206.1.1.5.
- Next, navigate to **Show / Change Server List** and select **Easy-Servers** and then **Add Server**. You should export both the Web (www-http) and Mail (smtp) ports to one of the now free public addresses. Select **Service...** and from the resulting pop-up menu select **www-http**. In the resulting screen enter your Web server's address, 192.168.1.2 and the public address, for example, 206.1.1.2 and then select **ADD NAT SERVER**. Now return to **Add Server**, choose the **smtp** port and enter 192.168.1.3, your Mail server's IP address for the **Server Private IP Address**. You can decide if you want to present both your Web and Mail services as being on the same public address, 206.1.1.2, or if you prefer to have your Mail server appear to be at a different IP address, 206.1.1.3. For the sake of this example, alias both services to 206.1.1.2.

Now, as before, the PAT configuration will allow any user on the Netopia R310's LAN with an IP address in the range of 192.168.1.6 through 192.168.1.254 to initiate traffic flow to the Internet. Someone at the FTP server can access the Internet and the Internet can access all services of the FTP machine as if it were at 206.1.1.5. The router cannot directly communicate with the outside world. The only communication between the Web server and the Internet is through port 80, the web port, as if the server were located on a machine at IP address 206.1.1.2. Similarly, the only communication with the Mail server is through port 25, the SMTP port, as if it were located at IP address 206.1.1.2

IP subnets

The IP Subnets screen allows you to configure up to eight Ethernet IP subnets, one "primary" subnet and up to seven secondary subnets, by entering IP address/subnet mask pairs:



Note: You need not use this screen if you have only a single Ethernet IP subnet. In that case, you can continue to enter or edit the IP address and subnet mask for the single subnet on the IP Setup screen.

This screen displays up to eight rows of two editable columns, preceded by a row number between one and eight. If you have eight subnets configured, there will be eight rows on this screen. Otherwise, there will be one more row than the number of configured subnets. The last row will have the value 0.0.0.0 in both the IP address and subnet mask fields to indicate that you can edit the values in this row to configure an additional subnet. All eight row labels are always visible, regardless of the number of subnets configured.

- To add an IP subnet, enter the Netopia R310's IP address on the subnet in the **IP Address** field in a particular row and the subnet mask for the subnet in the **Subnet Mask** field in that row.

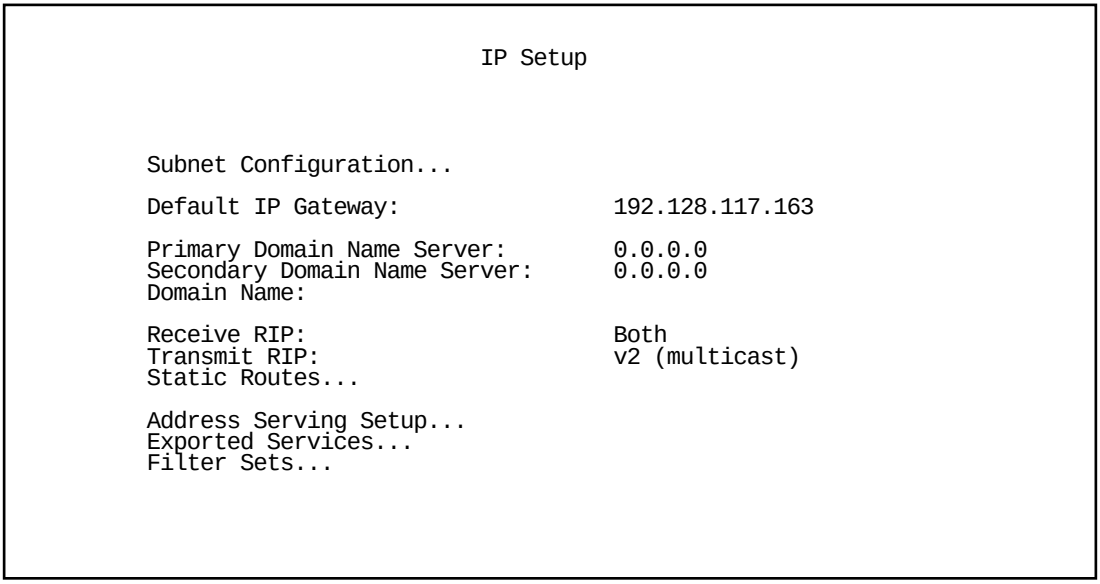
  For example:

```
                        IP Subnets

      IP Address          Subnet Mask
      ---------------     --------------
#1:   192.128.117.162     255.255.255.0
#2:   192.128.152.162     255.255.0.0
#3:   0.0.0.0             0.0.0.0
#4:
#5:
#6:
#7:
#8:
```

- To delete a configured subnet, set both the IP address and subnet mask values to 0.0.0.0, either explicitly or by clearing each field and pressing Return or Enter to commit the change. When a configured subnet is deleted, the values in subsequent rows adjust up to fill the vacant fields.

Note that the subnets configured on this screen are tied to the address serving pools configured on the IP Address Pools screen, and that changes on this screen may affect the IP Address Pools screen. In particular, deleting a subnet configured on this screen will delete the corresponding address serving pool, if any, on the IP Address Pools screen.

If you have configured multiple Ethernet IP subnets, the IP Setup screen changes slightly:



The IP address and Subnet mask items are hidden, and the "Define Additional Subnets..." item becomes "Subnet Configuration...". If you select **Subnet Configuration**, you will return to the IP Subnets screen that allows you to define IP addresses and masks for additional Ethernet IP subnets.

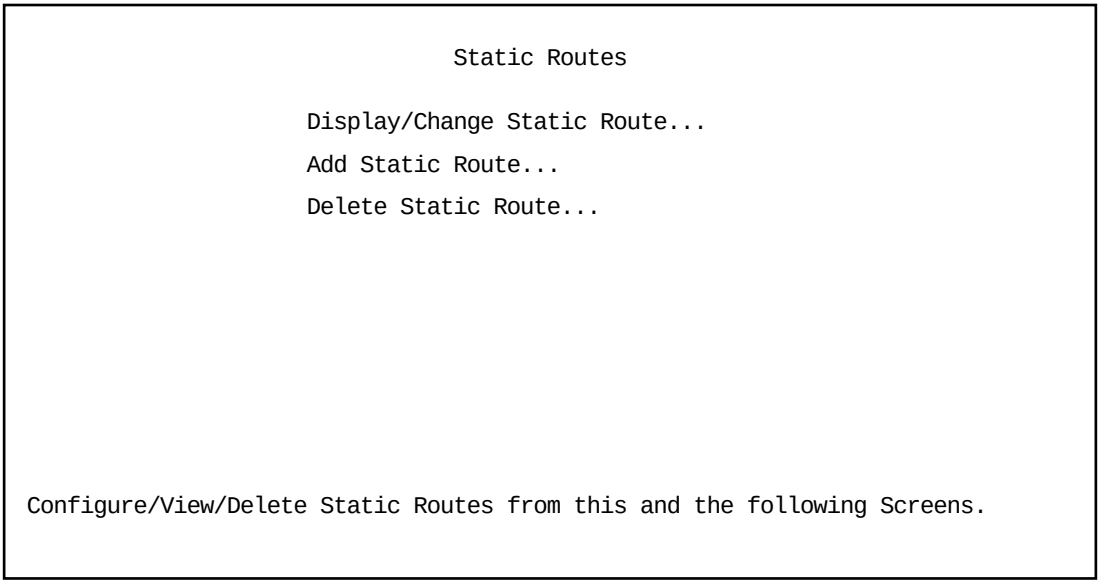
- Select **Static Routes** to manually configure IP routes. See the following section.

Static routes

Static routes are IP routes that are maintained manually. Each static route acts as a pointer that tells the Netopia R310 how to reach a particular network. However, static routes are used only if they appear in the IP routing table, which contains all of the routes used by the Netopia R310 (see "Routing tables" on page 11-7).

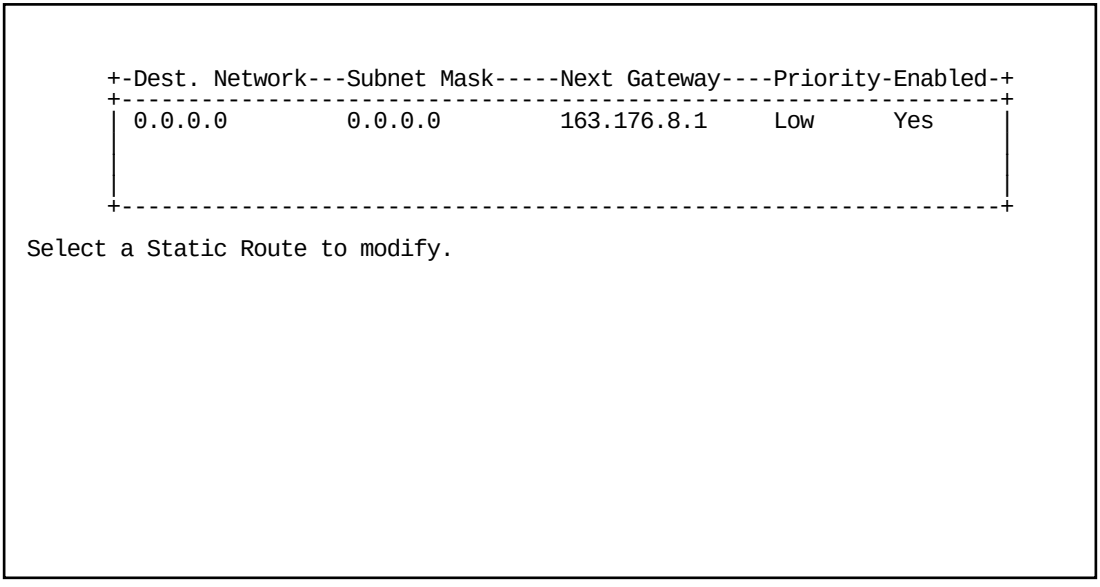
Static routes are helpful in situations where a route to a network must be used and other means of finding the route are unavailable. For example, static routes are useful when you cannot rely on RIP.

To go to the Static Routes screen, select the **Static Routes** item in the **IP Setup** screen.



Viewing static routes

To display a view-only table of static routes, select **Display / Change Static Route** in the Static Routes screen.



The table has the following columns:

Dest. Network: The network IP address of the destination network.

Subnet Mask: The subnet mask associated with the destination network.

Next Gateway: The IP address of the router that will be used to reach the destination network.

Priority: An indication whether the Netopia R310 will use the static route when it conflicts with information received from RIP packets.

Enabled: An indication whether the static route should be installed in the IP routing table.

Adding a static route

To add a new static route, select **Add Static Route** in the Static Routes screen and go to the Add Static Route screen.

```
                          Add Static Route

        Static Route Enabled:              Yes
        Destination Network IP Address:    0.0.0.0
        Destination Network Subnet Mask:   0.0.0.0
        Next Gateway IP Address:           0.0.0.0
        Route Priority...                  High
        Advertise Route Via RIP:           No



        ADD STATIC ROUTE NOW               CANCEL
Configure a new Static Route in this Screen.
```

- To install the static route in the IP routing table, select **Static Route Enabled** and toggle it to **Yes**. To remove the static route from the IP routing table, select **Static Route Enabled** and toggle it to **No**.
- Be sure to read the rules on the installation of static routes in the IP routing table. See "Rules of static route installation" on page 9-33.
- Select **Destination Network IP Address** and enter the network IP address of the destination network.
- Select **Destination Network Subnet Mask** and enter the subnet mask used by the destination network.
- Select **Next Gateway IP Address** and enter the IP address for the router that the Netopia R310 will use to reach the destination network. This router does not necessarily have to be part of the destination network, but it must at least know where to forward packets destined for that network.
- Select **Route Priority** and choose **High** or **Low**. **High** means that the static route takes precedence over RIP information; **Low** means that the RIP information takes precedence over the static route.
- If the static route conflicts with a connection profile, the connection profile will always take precedence.
- To make sure that the static route is known only to the Netopia R310, select **Advertise Route Via RIP** and toggle it to **No**. To allow other RIP-capable routers to know about the static route, select **Advertise Route Via RIP** and toggle it to **Yes**. When **Advertise Route Via RIP** is toggled to **Yes**, a new item called **RIP Metric** appears below **Advertise Route Via RIP**.

With **RIP Metric** you set the number of routers, from 1 to 15, between the sending router and the destination router. The maximum number of routers on a packet's route is 15. Setting **RIP Metric** to **1** means that a route can involve 15 routers, while setting it to **15** means a route can only involve one router.

- Select **ADD STATIC ROUTE NOW** to save the new static route, or select **CANCEL** to discard it and return to the Static Routes screen.
- Up to 32 static routes can be created, but one is always reserved for the default gateway, which is configured using either Easy Setup or the IP Setup screen in System Configuration.

Modifying a static route

To modify a static route, select **Display / Change Static Route** in the Static Routes screen to display a table of static routes.

Select a static route from the table and go to the Change Static Route screen. The parameters in this screen are the same as the ones in the Add Static Route screen (see "Adding a static route" on page 9-32).

Deleting a static route

To delete a static route, select **Delete Static Route** in the Static Routes screen to display a table of static routes. Select a static route from the table and press Return to delete it. To exit the table without deleting the selected static route, press the Escape key.

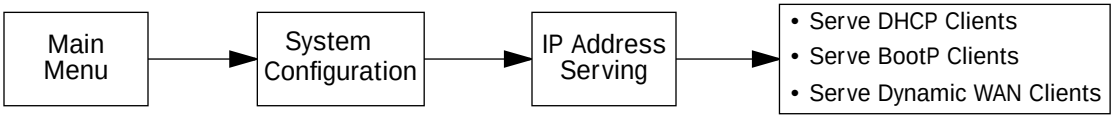
Rules of static route installation

The Netopia R310 applies certain rules before installing enabled static routes in the IP routing table. An enabled static route will not be installed in the IP routing table if any of the following conditions are true:

- The static route's **Next Gateway IP Address** matches the IP address used by a connection profile or the Netopia R310's Ethernet port.
- The static route's **Next Gateway IP Address** matches an IP address in the range of IP addresses being distributed by MacIP or DHCP.
- The static route's **Next Gateway IP Address** is determined to be unreachable by the Netopia R310.
- The static route's route information conflicts with a connection profile's route information.
- The connection profile associated with the static route is set for dial-in connections only, and there is no incoming call connected to that connection profile.
- The connection profile associated with the static route has a disabled dial-on-demand setting, and there is no current connection using that connection profile.

A static route is already installed in the IP routing table will be removed if any of the conditions listed above become true for that static route. However, an enabled static route is automatically reinstalled once the conditions listed above are no longer true for that static route.

IP address serving



In addition to being a router, the Netopia R310 is also an IP address server. There are three protocols it can use to distribute IP addresses.

- The first, called **Dynamic Host Configuration Protocol (DHCP)**, is widely supported on PC networks, as well as Apple Macintosh computers using Open Transport and computers using the UNIX operating system. Addresses assigned via DHCP are "leased" or allocated for a short period of time; if a lease is not renewed, the address becomes available for use by another computer. DHCP also allows most of the IP parameters for a computer to be configured by the DHCP server, simplifying setup of each machine.
- The second, called **BOOTP** (also known as Bootstrap Protocol), is the predecessor to DHCP and allows older IP hosts to obtain most of the information that a DHCP client would obtain. However, in contrast, BOOTP address assignments are "permanent" since there is no lease renewal mechanism in BOOTP.
- The third protocol, called **Dynamic WAN**, is part of the PPP/MP suite of wide area protocols used for WAN connections. It allows remote terminal adapters and NAT-enabled routers to be assigned a temporary IP address for the duration of their connection.

Since no two hosts can use the same IP address at the same time, make sure that the addresses distributed by the Netopia R310 and those that are manually configured are not the same. Each method of distribution must have its own exclusive range of addresses to draw from.

To go to the IP Address Serving screen, select **IP Address Serving** in the System Configuration screen and press Return.

```
                          IP Address Serving

        IP Address Serving Mode...          DHCP Server

        Number of Client IP Addresses:      100
        1st Client Address:                 192.168.1.100
        Client Default Gateway...           192.168.1.1


        Serve DHCP Clients:                 Yes
        DHCP Lease Time (Hours):            1
        DHCP NetBIOS Options...

        Serve BOOTP Clients:                Yes

        Serve Dynamic WAN Clients           Yes



Configure Address Serving (DHCP, BOOTP, etc.) here.
```

Follow these steps to configure IP Address Serving:

- If you enabled IP Address Serving either by using SmartStart or in Easy Setup, DHCP, BootP clients, and Dynamic WAN clients are automatically enabled.
- Select **Number of Client IP Addresses** and enter the total number of contiguous IP addresses that the Netopia R310 will distribute to the client machines on your local area network.
- In the screen example shown above, a hundred Client IP addresses have been allocated.
- Select **1st Client Address** and enter the first client IP address that you will allocate to your first client machine. For instance, on your local area network you may first want to figure out what machines are going to be allocated specific static IP addresses so that you can determine the pool of IP addresses that you will be serving addresses from via DHCP, BOOTP, and/or Dynamic WAN.

  Note: On a Netopia R310 the factory default IP Address serving settings are:

  1st Client Address: 192.168.1.3

  Number of Client IP Addresses: 100

  (this allows for one static address at 192.168.1.2 for the server)
- **Example:** Your ISP has given your Netopia R310 the IP address 192.168.6.137, with a subnet mask of 255.255.255.248. The subnet mask allocated will give you six IP addresses to use when connecting to the ISP over the Internet (for more information on understanding IP addressing refer to Appendix D, "Understanding IP Addressing."). Your address range will be from **.137-.143**. In this example you would enter **192.168.6.138** as the 1st client address, as the router itself must have an IP address.
- To enable DHCP, select **Serve DHCP Clients** and toggle it to **Yes**. DHCP serving is automatic when IP Address Serving is enabled.

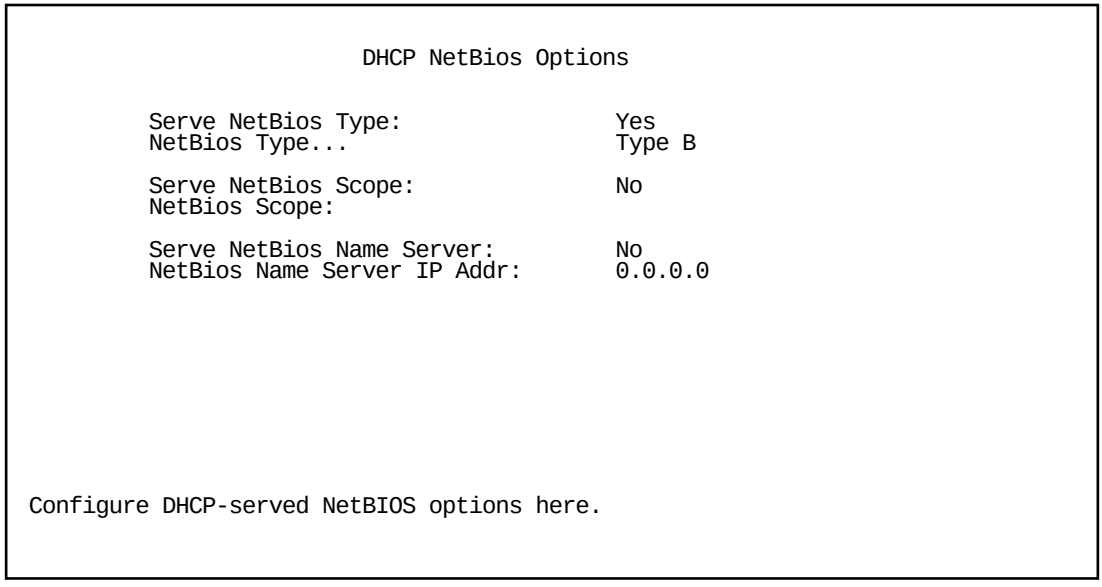
  Note: When the remote router requests a DNS server address via IPCP, the Netopia R310 will supply whatever DNS address that is either manually configured or acquired dynamically. This feature allows a DNS to be served that was acquired via DHCP.
- The Netopia R310 defaults to a DHCP lease time of one hour. If this is unnecessarily brief for your network environment, you can configure the **DHCP Lease Time (Hours)** field. You can enter any number up to and including 168 (one week) for the DHCP lease.

DHCP NetBIOS Options

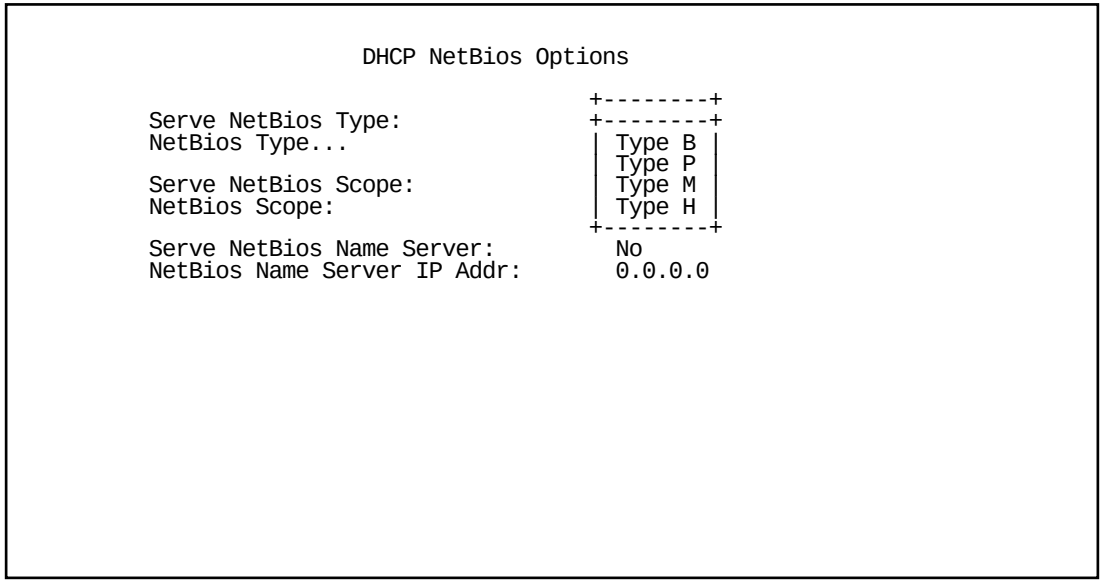
If your network uses NetBIOS, you can enable the Netopia R310 to use DHCP to distribute NetBIOS information.

NetBIOS stands for Network Basic Input/Output System. It is a layer of software originally developed by IBM and Sytek to link a network operating system with specific hardware. NetBIOS has been adopted as an industry standard. It offers LAN applications, a variety of "hooks" to carry out inter-application communications and data transfer. Essentially, NetBIOS is a way for application programs to talk to the network. To run an application that works with NetBIOS, a non-IBM network operating system or network interface card must offer a NetBIOS emulator. Many vendors either provide a version of NetBIOS to interface with their hardware or emulate its transport layer communications services in their network products. A NetBIOS emulator is a program provided by NetWare clients that allow workstations to run applications that support IBM's NetBIOS calls.

- Select **Serve NetBIOS Options** and press Return. The DHCP NetBIOS Options screen appears.



- To serve DHCP clients with the type of NetBIOS used on your network, select **Serve NetBIOS Type** and toggle it to **Yes**.
- From the **NetBIOS Type** pop-up menu, select the type of NetBIOS used on your network.



- To serve DHCP clients with the NetBIOS scope, select **Serve NetBIOS Scope** and toggle it to **Yes**.

  Select **NetBIOS Scope** and enter the scope.
- To serve DHCP clients with the IP address of a NetBIOS name server, select **Serve NetBIOS Name Server** and toggle it to **Yes**.

Select **NetBIOS Name Server IP Address** and enter the IP address for the NetBIOS name server.

You are now finished setting up DHCP NetBIOS Options. To return to the IP Address Serving screen press the Escape key once.

- To enable BootP's address serving capability, select **Serve BOOTP Clients** and toggle to **Yes**.

  Note: Addresses assigned through BOOTP are permanently allocated from the IP Address Serving pool until you release them. To release these addresses, navigate back to the Main Menu, then Statistics & Logs, Served IP Addresses, and **Lease Management**. See "Served IP Addresses" on page 11-8.

You have finished your IP Setup.

Chapter 10

Virtual Private Networks (VPN)

The Netopia R310 Router offers both PPTP and ATMP tunneling support for Virtual Private Networks (VPN).

Note: VPN is an optional add-on to the Netopia R310. Order TER/VPN2 from the Netopia Web site at www.netopia.com or from your Netopia reseller.

The following topics are covered in this chapter:

Overview

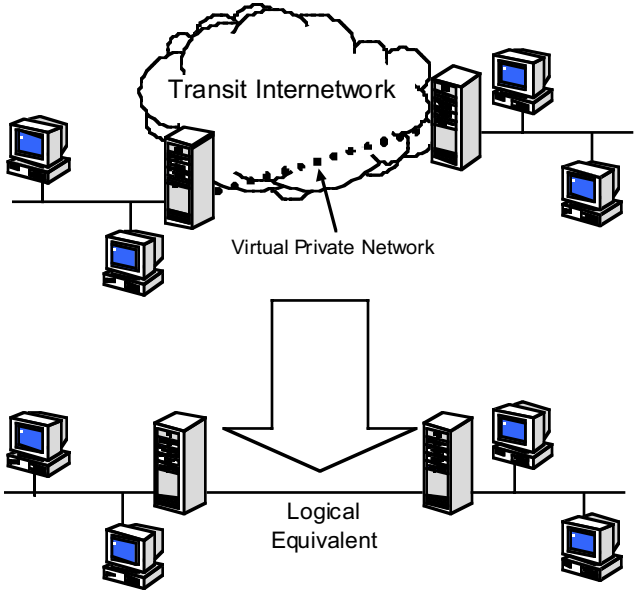
When you make a long distance telephone call from your home to a relative far away, you are creating a private network. You can hold a conversation, and exchange information about the happenings on opposite sides of the country, or the continent, that you are mutually interested in. When your next door neighbor picks up the phone to call her daughter at college, at the same time you are talking to your relatives, your calls don't overlap, but each is separate and private. Neither house has a direct wire to the places they call. Both share the same lines on the telephone poles (or underground) on the street.

These calls are *virtual private networks*. *Virtual*, because they appear to be direct connections between the calling and answering parties, even though they travel over the public wires and switches of the phone company; *private*, because neither pair of calling and answering parties interacts with the other; and *networks*, because they exchange information.

Computers can do the same thing; it's called Virtual Private Networks (VPNs). Equipped with Netopia R310s, a single computer or private network (LAN) can establish a private connection with another computer or private network over the public network (Internet).

The Netopia R310 can be used in VPNs either to initiate the connection or to answer it. When used in this way, the routers are said to be *tunnelling* through the public network (Internet). The advantages are that, like your long distance phone call, you don't need a direct line between one computer or LAN and the other, but use the local connections, making it much cheaper; and the information you exchange through your tunnel is private and secure.

Tunneling is a process of creating a private path between a remote user or private network and another private network over some intermediate network, such as the IP-based Internet. A VPN allows remote offices or employees access to your internal business LAN through means of encryption allowing the use of the public Internet to look "virtually" like a private secure network. When two networks communicate with each other through a network based on the Internet Protocol, they are said to be *tunneling* through the IP network.



Unlike the phone company, private and public computer networks can use more than one protocol to carry your information over the wires. Two such protocols are in common use for tunnelling, Point-to-Point Tunnelling Protocol (PPTP) and Ascend Tunnel Management Protocol (ATMP). The Netopia R310 can use either one.

- Point-to-Point Tunneling Protocol (PPTP) is an extension of Point-to-Point Protocol (PPP) and uses a client and server model. Netopia's PPTP implementation is compatible with Microsoft's and can function as either the client (PAC) or the server (PNS). As a client, a Netopia R-series router can provide all users on a LAN with secure access over the Internet to the resources of another LAN by setting up a tunnel with a Windows NT server running Remote Access Services (RAS) or with another Netopia Router. As a server, a Netopia R-series router can provide remote users a secure connection to the resources of the LAN over a dial-up, cable, DSL, or any other type of Internet access. Because PPTP can create a VPN tunnel using the Dial-Up Networking (DUN) (see "Dial-Up Networking for VPN" on page 10-10) utility built into Windows 95, 98, or NT, no additional client software is required.
- Ascend Tunnel Management Protocol (ATMP) is the protocol that is implemented in many Ascend routers. ATMP is a simple protocol for connecting nodes and/or networks together over the Internet via a tunnel. ATMP encapsulates IP or other user data without PPP headers within General Routing Encapsulation (GRE) protocol over IP. ATMP is more efficient than PPTP for network-to-network tunnels.

When used to initiate the tunnelled connection, the Netopia R310 is called a *PPTP Access Concentrator* (*PAC*, in PPTP language), or a *foreign agent* (in ATMP language). When used to answer the tunnelled connection, the Netopia R310 is called a *PPTP Network Server* (*PNS*, in PPTP language) or a *home agent* (in ATMP language).

In either case, the Netopia R310 wraps, or encapsulates, information that one end of the tunnel exchanges with the other, in a wrapper called General Routing Encapsulation (GRE), at one end of the tunnel, and unwraps, or decapsulates, it at the other end.

Configuring the Netopia R310 for use with either of the two protocols is done through the console-based menu screens. Each type is described in its own section:

- "About PPTP Tunnels" on page 10-4
- "About ATMP Tunnels" on page 10-16

Your configuration depends on which protocol you (and the router at the other end of your tunnel) will use, and whether or not you will be using the VPN client software in a standalone remote connection.

Note: You must choose which protocol you will be using, since you cannot both export PPTP and use ATMP, or vice versa, at the same time.

Having both an ATMP tunnel and a PPTP export is not possible because functions require GRE and the router's PPTP export/server does not distinguish the GRE packets it forwards. Since it processes all of them, ATMP tunneling is impaired. For example, you cannot run an ATMP tunnel between two routers and also have PPTP exported on one side.

Summary

A Virtual Private Network (VPN) connects the components of one network over another network. VPNs accomplish this by allowing you to *tunnel* through the Internet or another public network in a manner that provides the same security and features formerly available only in private networks.

VPNs allow networks to communicate across an IP network. Your local networks (connected to the Netopia R310) can exchange data with remote networks that are also connected to a VPN-capable router.

This feature provides individuals at home, on the road, or in branch offices with a cost-effective and secure way to access resources on remote LANs connected to the Internet with Netopia Routers. The feature is built around two key technologies: PPTP and ATMP.

About PPTP Tunnels

To set up a PPTP tunnel, you create a Connection Profile including the IP address and other relevant information for the remote PPTP partner. You use the same procedure to initiate a PPTP tunnel that terminates at a remote PPTP server or to terminate a tunnel initiated by a remote PPTP client.

PPTP configuration

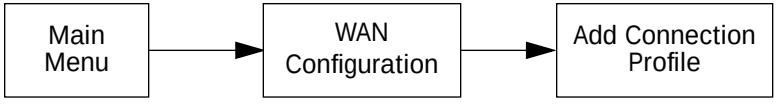
To set up the router as a PPTP Network Server (PNS) capable of answering PPTP tunnel requests you must also configure the VPN Default Answer Profile. See “VPN Default Answer Profile” on page 10-8 for more information.

PPTP is a Datalink Encapsulation option in Connection Profiles. It is not an option in device or link configuration screens, as PPTP is not a native encapsulation. Consequently, the Easy Setup Profile does not offer PPTP datalink encapsulation. See “Creating a new Connection Profile” on page 7-1 for information on creating Connection Profiles.

Note: As of firmware version 4.4, the R9100 Ethernet-to-Ethernet Router now has access to Connection Profiles for tunnelling purposes. If the PPP dialup kit is not installed you cannot use PPP as a datalink encapsulation, and you will have access only to ATMP and PPTP. If the kit is installed you also have access to PPP.

Channel 4 (and higher) events, such as connections and disconnections, reported in the WAN Event Histories are VPN tunnel events.

To define a PPTP tunnel, navigate to the Add Connection Profile menu from the Main Menu.




```
                    Add Connection Profile

Profile Name:                      Profile 2
Profile Enabled:                 +-------------+
                                 +-------------+
Data Link Encapsulation...       | PPP         |
Data Link Options...             | ATM FUNI    |
                                 | ATMP        |
IP Enabled:                      | PPTP        |
IP Profile Parameters...         +-------------+









ADD PROFILE NOW                    CANCEL
```

When you define a Connection Profile as using PPTP by selecting PPTP as the datalink encapsulation method, and then select **Data Link Options**, the PPTP Tunnel Options screen appears.

```
                          PPTP Tunnel Options

        PPTP Partner IP Address:          173.167.8.134
        Tunnel Via Gateway:               0.0.0.0

        Data Compression...               None
        Authentication...                 CHAP


        Send Host name:                   tony
        Send Secret:                      *****

        Receive Host name:                kimba
        Receive Secret:                   ******


        Initiate Connections:             Yes
        On Demand:                        Yes

        Idle Timeout (seconds):           300

Return accepts * ESC cancels * Left/Right moves insertion point * Del deletes.
In this Screen you will configure the GRE/PPTP specific connection params.
```

Note: Profiles using PPTP do not offer a Telco Options screen.

- Enter the **PPTP Partner IP Address**. This specifies the address of the other end of the tunnel.

  If you do not specify the PPTP Partner IP Address the gateway cannot initiate tunnels, i.e., act as a PPTP Access Concentrator (PAC) for this profile. It can only accept tunnel requests as a PPTP Network Server (PNS).

- If you specify the PPTP Partner IP Address, and the address is in the same subnet as the Remote IP Address you specified in the IP Profile Parameters, the **Tunnel Via Gateway** option becomes visible. You can enter the address by which the gateway partner is reached.

  If you do not specify the PPTP Partner IP Address, the router will use the default gateway to reach the partner and the **Tunnel Via Gateway** field is hidden. If the partner should be reached via an alternate port (i.e. the LAN instead of the WAN), the **Tunnel Via Gateway** field allows this path to be resolved.

- You can specify a **Data Compression** algorithm, either None or Standard LZS, for the PPTP connection.

  Note: When the Authentication protocol is MS-CHAP, compression is set to None, and the **Data Compression** option is hidden.

- From the pop-up menu select an **Authentication** protocol for the PPP connection. Options are PAP, CHAP, or MS-CHAP. The default is PAP. The authentication protocol must be the same on both ends of the tunnel.

- When the authentication protocol is MS-CHAP, you can specify a **Data Encryption** algorithm for the PPTP connection. Available options are MPPE and None (the default). For other authentication protocols, this option is hidden. When MPPE is negotiated, the WAN Event History reports that it is negotiated as a CCP (compression) type. This is because the MPPE protocol uses a compression engine, even though it is not itself a compression protocol.

- You can specify a **Send Host Name** which is used with Send Secret for authenticating with a remote PNS when the profile is used for initiating a tunnel connection.
- You must specify a **Send Secret** (the CHAP term for password), used for authenticating the tunnel when initiating a tunnel connection.
- You can specify a **Receive Host Name** which is used with the Receive Secret for authenticating a remote PPTP client.
- You must specify a **Receive Secret**, used for authenticating the remote PPTP client.
- You can specify that this router will **Initiate Connections** (acting as a PAC) or only answer them (acting as a PNS).
- Tunnels are normally initiated **On Demand**; however, you can disable this feature. When disabled, the tunnel must be manually established via the call management screens or may be scheduled using the scheduled connections feature. See "Scheduled Connections" in the *User's Reference Guide*.
- You can specify the **Idle Timeout**, an inactivity timer, whose expiration will terminate the tunnel. A value of zero disables the timer. Because tunnels are subject to abrupt termination when the underlying datalink is torn down, use of the Idle Timeout is strongly encouraged.

  An alternate way to force a tunnel to stay up is to define a forced up scheduled connection for the profile.
- Return to the Connection Profile screen by pressing Escape.
- Select **IP Profile Parameters** and press Return.

  The IP Profile Parameters screen appears.

```
                          IP Profile Parameters

        Address Translation Enabled:       Yes

        NAT Map List...                    Easy-PAT
        NAT Server List...                 Easy-Servers

        Local WAN IP Address:              0.0.0.0

        Remote IP Address:                 173.167.8.10
        Remote IP Mask:                    255.255.0.0

        Filter Set...
        Remove Filter Set

        Receive RIP:                       Both


Enter a subnet mask in decimal and dot form (xxx.xxx.xxx.xxx).
```

- Enter the **Remote IP Address** and **Remote IP Mask** for the host to which you want to tunnel.

Note: A peculiarity associated with VPNs is that when a PAC has NAT applied to a Connection Profile set for PPTP data link encapsulation, the PNS and devices behind it, cannot Ping the PAC's tunnel end-point IP address. This is because ICMP packets have no port association, and thus will be discarded rather than being processed by NAT.

Ordinarily, Ping is an excellent troubleshooting tool, but it will not be effective in this circumstance. Instead, use another TCP- or UDP-based network service for troubleshooting. Since the Netopia R310 is capable of serving Telnet and HTTP, we recommend using these services instead of Ping.

Encryption Support

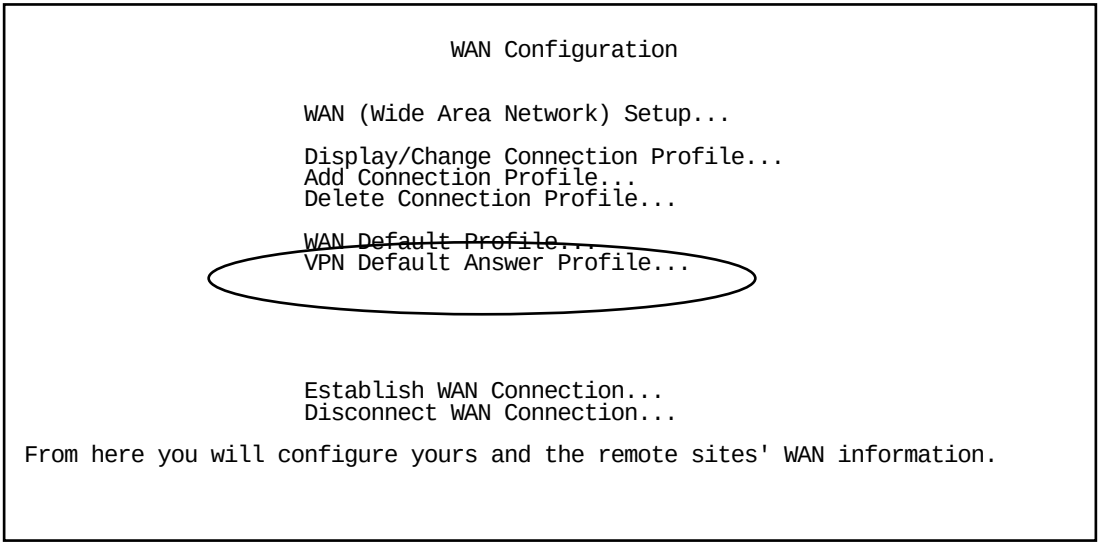
Encryption is a method for altering user data into a form that is unusable by anyone other than the intended recipient. The recipient must have the means to decrypt the data to render it usable to them. The encryption process protects the data by making it difficult for any third party to get at the original data.

Netopia PPTP is fully compatible with Microsoft Point-to-Point Encryption (MPPE) data encryption for user data transfer over the PPTP tunnel. Microsoft Windows NT Server provides MPPE encryption capability only when Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) is enabled. Netopia complies with this feature to allow MPPE only when MS-CHAP is negotiated. MS-CHAP and MPPE are user-selectable options in the PPTP Tunnel Options screen. If either the client or the server side specifies encryption, then encryption becomes mandatory for both.

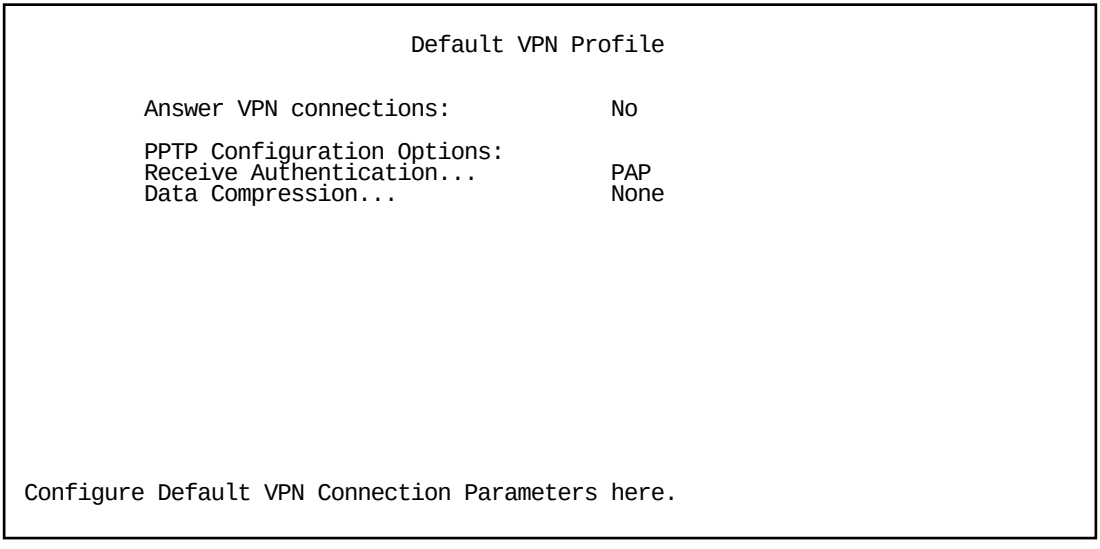
Netopia's ATMP implementation supports Data Encryption Standard (DES) data encryption for user data transfer over the ATMP tunnel between two Netopia routers. The encryption option, none or DES, is a selectable option in the ATMP Tunnel Options screen.

VPN Default Answer Profile

The WAN Configuration menu offers a VPN Default Answer Profile option. Use this selection when your router is acting as the server for VPN connections, that is, when you are on the answering end of the tunnel establishment. The VPN Default Answer Profile determines the way the attempted tunnel connection is answered.



To set the parameters under which the router will answer attempted VPN connections, select **VPN Default Answer Profile** and press Return. The Default VPN Profile screen appears.



- Toggle **Answer VPN Connections** to **Yes** if you want the router to accept VPN connections or **No** (the default) if you do not. This applies to both ATMP and PPTP connections.

- For PPTP tunnel connections only, you must define what type of authentication these connections will use. Select **Receive Authentication** and press Return. A pop-up menu offers the following options: PAP (the default), CHAP, or MS-CHAP.
- If you chose PAP or CHAP authentication, from the **Data Compression** pop-up menu select either None (the default) or Standard LZS.

  If you chose MS-CHAP authentication, the **Data Compression** option is not required, and this menu item becomes hidden.

VPN QuickView

You can view the status of your VPN connections in the VPN QuickView screen.

From the Main Menu select QuickView and then VPN QuickView.

The VPN QuickView screen appears.

```
                              VPN Quick View

Profile Name----------Type--Rx Pckts--Tx Pckts------Est.-Partner Address------
HA <-> FA1 (Jony Fon  ATMP        99        99      Rmt  173.166.82.8
HA <-> FA3 (Sleve M.  ATMP        13        14      Rmt  63.193.117.91
```

Profile Name: Lists the name of the Connection Profile being used, if any.

Type: Shows the data link encapsulation method (PPTP or ATMP).

Rx Pckts: Shows the number of packets received via the VPN tunnel.

Tx Pckts: Shows the number of packets transmitted via the VPN tunnel.

Est: Indicates whether the connection was locally (“Lcl”) or remotely (“Rmt”) established.

Partner Address: Shows the tunnel partner’s IP address.

Dial-Up Networking for VPN

Microsoft Windows Dial-Up Networking software permits a remote standalone workstation to establish a VPN tunnel to a PPTP server such as a Netopia R310 located at a central site. Dial-Up Networking also allows a mobile user who may not be connected to a PAC to dial into an intermediate ISP and establish a VPN tunnel to, for example, a corporate headquarters, remotely. Netopia Routers also can serve as a PAC at the workstation's site, making it unnecessary for the standalone workstation to initiate the tunnel. In such a case, the Dial-Up Networking software is not required, since the Netopia R310 initiates the tunnel.

This section is provided for users who may require the VPN client software for Dial-Up Networking in order to connect to an ISP who provides a PPTP account.

Microsoft Windows Dial-Up Networking (DUN) is the means by which you can initiate a VPN tunnel between your individual remote client workstation and a private network such as your corporate LAN via the Internet. DUN is a software adapter that allows you to establish a tunnel.

DUN is a free add-on available for Windows 95, and comes standard with Windows 98 and Windows NT. The VPN tunnel behaves as a private network connection, unrelated to other traffic on the network. Once you have installed Dial-Up Networking, you will be able to connect to your remote site as if you had a direct private connection, regardless of the intervening network(s) through which your data passes. You may need to install the Dial-Up Networking feature of Windows 95, 98, or 2000 to take advantage of the virtual private networking feature of your Netopia R310.

Note: For the latest information and tech notes on Dial-Up Networking and VPNs be sure to visit the Netopia website at http://www.netopia.com and, for the latest software and release notes, the Microsoft website at http://www.microsoft.com.

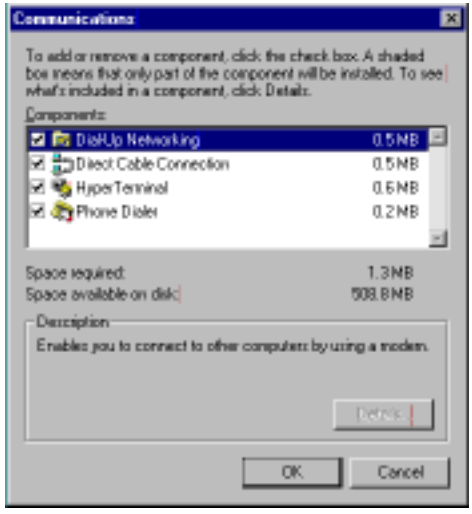
Installing Dial-Up Networking

Check to see if Dial-Up Networking is already installed on your PC. Open your My Computer (or whatever you have named it) icon on your desktop. If there is a folder named Dial-Up Networking, you don't have to install it. If there is no such folder, you must install it from your system disks or CDROM. Do the following:

1. From the **Start** menu, select **Settings** and then **Control Panel**.
2. In the Control Panel window, double-click the **Add/Remove Programs** icon.

   The Add/Remove Programs Properties window appears.
3. Click the **Windows Setup** tab.
4. Double-click **Communications**.

The Communications window appears.



5. In the Communications window, select **Dial-Up Networking** and click the **OK** button.

   This returns you to the Windows Setup screen. Click the **OK** button.

6. Respond to the prompts to install Dial-Up Networking from the system disks or CDROM.

7. When prompted, reboot your PC.

Creating a new Dial-Up Networking profile

A Dial-Up Networking profile is like an address book entry that contains the information and parameters you need for a secure private connection. You can create this profile by using either the Internet Connection Wizard or the Make New Connection feature of Dial-Up Networking. The following instructions tell you how to create the profile with the Make New Connection feature. Do the following:

1. Double-click the **My Computer** (or whatever you have named it) icon on your desktop.

   Open the Dial-Up Networking folder, and then double-click **Make New Connection**. The Make New Connection wizard window appears.

2. Type a name for this connection (such as the name of your company, or the computer you are dialing into).

   From the pull-down menu, select the device you intend to use for the virtual private network connection. This can be any device you have installed or connected to your PC. Click the **Next** button. A screen appears with fields for you to enter telephone numbers for the computer you want to connect to.

3. Type the directory number or the **Virtual Circuit Identifier** number.

   This number is provided by your ISP or corporate administrator. Depending on the type of device you are using, the number may or may not resemble an ordinary telephone directory number.

4. Click the **Next** button.

   The final window will give you a chance to accept or change the name you have entered for this profile. If you are satisfied with it, click the **Finish** button. Your profile is complete.

Configuring a Dial-Up Networking profile

Once you have created your Dial-Up Networking profile, you configure it for TCP/IP networking to allow you to connect to the Internet through your Internet connection device. Do the following:

1. Double-click the **My Computer** (or whatever you have named it) icon on your desktop.

   Open the Dial-Up Networking folder. You will see the icon for the profile you created in the previous section.

2. Right-click the icon and from the pop-up menu select **Properties**.

3. In the Properties window click the **Server Type** button.

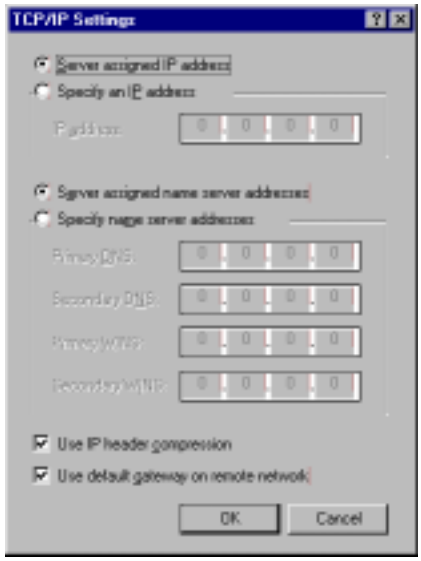
   From the Type of Dial-up Server pull-down menu select the appropriate type of server for your system version:

- Windows 95 users select **PPP: Windows 95, Windows NT 3.5, Internet**
- Windows 98 users select **PPP: Windows 98, Windows NT Server, Internet**

In the Allowed network protocols area check **TCP/IP** and uncheck all of the other checkboxes.

Note: Netopia's PPTP implementation does not currently support tunnelling of IPX and NetBEUI protocols.

4. Click the **TCP / IP Settings** button.



- If your ISP uses dynamic IP addressing (DHCP), select the Server assigned IP address radio button.
- If your ISP uses static IP addressing, select the Specify an IP address radio button and enter your assigned IP address in the fields provided. Also enter the IP address in the Primary and Secondary DNS fields.

5. Click the **OK** button in this window and the next two windows.

Installing the VPN Client

Before Installing the VPN Client you must have TCP/IP installed and have an established Internet connection.

Windows 95 VPN installation

1. From your Internet browser navigate to the following URL:

   http://www.microsoft.com/NTServer/nts/downloads/recommended/dunl3win95/releasenotes.aso

   Download the Microsoft Windows 95 VPN patch dun 1.3 to the Windows 95 computer you intend to use as a VPN client with PPTP. Follow the installation instructions.

2. From the Windows 95 **Start** menu select **Settings**, then **Control Panel** and click once.

   The Control Panel screen appears.

3. Double-click **Add/Remove Programs**.

   The Add/Remove Programs screen appears.

4. Click the **Windows Setup** tab.

   The Windows Setup screen will be displayed within the top center box.

5. Highlight **Communications** and double-click.

   This displays a list of possible selections for the communications option. Active components will have a check in the checkboxes to their left.

6. Check **Dial Up Networking** at the top of the list and **Virtual Private Networking** at the bottom of the list.

7. Click **OK** at the bottom right on each screen until you return to the Control Panel. Close the Control Panel by clicking the upper right corner X.

8. Double-click the **My Computer** icon (normally at the left upper corner of the screen).

   This will display the devices within My Computer. Scroll down the list to **Dial-Up Networking** and double-click it.

9. Double click **Make New Connection**.

   This displays the Make New Connection installation screen. In this screen you will see a box labelled **Select a device**. From the pull-down menu to the right, select **Microsoft VPN Adapter**.

   Click the **Next** button at the bottom of the screen

   This displays the **VPN Host** screen. In the box to the top center of the screen enter your VPN server's IP address (for example, 192.168.xxx.xxx. This is not a proper Internet address)

Windows 98 VPN installation

1. From the Windows 98 **Start** menu select **Settings**, then **Control Panel** and click once.

   The Control Panel screen appears.

2. Double-click **Add/Remove Programs**.

   The Add/Remove Programs screen appears.

3. Click the **Windows Setup** tab.

   The Windows Setup screen will be displayed within the top center box.

4. Double-click **Communications**.

   This displays a list of possible selections for the communications option. Active components will have a check in the checkboxes to their left.

5. Check **Dial Up Networking** at the top of the list and **Virtual Private Networking** at the bottom of the list.

6. Click **OK** at the bottom right on each screen until you return to the Control Panel. Close the Control Panel by clicking the upper right corner X.

7. Double-click the **My Computer** icon (normally at the left upper corner of the screen).

   This will display the devices within My Computer. Scroll down the list to **Dial-Up Networking** and double-click it.

8. Double click **Make New Connection**.

   This displays the Make New Connection installation screen. In this screen you will see a box labelled **Select a device**. From the pull-down menu to the right, select **Microsoft VPN Adapter**.

   Click the **Next** button at the bottom of the screen

   This displays the **VPN Host** screen. In the box to the top center of the screen enter your VPN server's IP address (for example, 192.168.xxx.xxx. This is not a proper Internet address)

Connecting using Dial-Up Networking

A Dial-Up Networking connection will be automatically launched whenever you run a TCP/IP application, such as a web browser or email client. When you first run the application a Connect To dialog box appears in which you enter your User name and Password. If you check the Save password checkbox, the system will remember your User name and Password, and you won't be prompted for them again.

About ATMP Tunnels

To set up an ATMP tunnel, you create a Connection Profile including the IP address and other relevant information for the remote ATMP partner. ATMP uses the terminology of a *foreign agent* that initiates tunnels and a *home agent* that terminates them. You use the same procedure to initiate or terminate an ATMP tunnel. Used in this way, the terms *initiate* and *terminate* mean the beginning and end of the tunnel; they do not mean *activate* and *deactivate*.

ATMP is a tunneling protocol, with two basic aspects. Tunnels are created and torn down using a session protocol that is UDP-based. User (or client) data is transferred across the tunnel by encapsulating the client data within Generic Routing Encapsulation (GRE). The GRE data is then routed using standard methods.

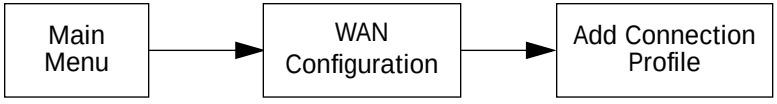
ATMP configuration

ATMP is a Datalink Encapsulation option in Connection Profiles. It is not an option in device or link configuration screens, since ATMP is not a native encapsulation. The Easy Setup Profile does not offer ATMP datalink encapsulation. See “Creating a new Connection Profile” on page 7-1 for information on creating Connection Profiles.

Note: The R9100 Ethernet-to-Ethernet Router now has access to Connection Profiles for tunnelling purposes. If the PPP dialup kit is not installed you cannot use PPP as a datalink encapsulation, and have access only to ATMP and PPTP. If the kit is installed you also have access to PPP.

The WAN Event History screens will report VPN tunnel events, such as connections and disconnections, as Channel 4 (and higher) events.

To define an ATMP tunnel, navigate to the **Add Connection Profile** menu from the Main Menu.



```
                        Add Connection Profile

        Profile Name:                     Profile 1
        Profile Enabled:                +-------------+
                                        +-------------+
        Data Link Encapsulation...      | PPP         |
        Data Link Options...            | ATM FUNI    |
                                        | ATMP        |
        IP Enabled:                     | PPTP        |
        IP Profile Parameters...        +-------------+









        ADD PROFILE NOW                   CANCEL
```

When you define a Connection Profile as using ATMP by selecting ATMP as the datalink encapsulation method, and then select **Data Link Options**, the ATMP Tunnel Options screen appears.

```
                        ATMP Tunnel Options


        ATMP Partner IP Address:          173.167.8.134
        Tunnel Via Gateway:               0.0.0.0

        Network Name:                     sam.net
        Password:                         ****

        Data Encryption...                DES
        Key String:

        Initiate Connections:             Yes
        On Demand:                        Yes

        Idle Timeout (seconds):           300




Enter an IP address in decimal and dot form (xxx.xxx.xxx.xxx).
In this Screen you will configure the GRE/ATMP specific connection params.
```

Note: An ATMP tunnel cannot be assigned a dynamic IP address by the remote server, as in a PPP connection. When you define an ATMP tunnel profile, the Local WAN IP Address, assigned in the IP Profile Parameters screen, must be the true IP address, not 0.0.0.0, if NAT is enabled.

Note: Profiles using ATMP do not offer a Telco Options screen.

- **ATMP Partner IP Address** specifies the address of the other end of the tunnel. When unspecified, the gateway can not initiate tunnels (i.e., act as a foreign agent) for this profile; it can only accept tunnel requests as a home agent.

- When you specify the ATMP Partner IP Address, and the address is in the same subnet as the Remote IP Address you specified in the IP Profile Parameters, you can specify the route (**Tunnel Via Gateway**) by which the gateway partner is reached. If you do not specify the ATMP Partner IP Address, the router will use the default gateway to reach the partner and the **Tunnel Via Gateway** field is hidden. If the partner should be reached via an alternate port (i.e., the LAN instead of the WAN), the **Tunnel Via Gateway** field allows this path to be resolved.
- You can specify a **Network Name**. When the tunnel partner is another Netopia R310, this name may be used to match against a Connection Profile. When the partner is an Ascend router in Gateway mode, then **Network Name** is used by the Ascend router to match a gateway profile. When the partner is an Ascend router in Router mode, leave this field blank.
- You must specify a **Password**, used for authenticating the tunnel.

  Note: The Password entry will be the same for both ends of the tunnel.
- For Netopia-to-Netopia connections only, you can specify a **Data Encryption** algorithm for the ATMP connection from the pop-up menu, either DES or None. None is the default.

  Note: Ascend does not support DES encryption for ATMP tunnels.
- You must specify an 8-byte **Key String** when DES is selected. When encryption is None, this field is invisible.
- You can specify that this router will **Initiate Connections**, acting as a foreign agent (**Yes**), or only answer them, acting as a home agent (**No**).
- Tunnels are normally initiated **On Demand**; however, you can disable this feature. When disabled, the tunnel must be manually established through the call management screens.
- You can specify the **Idle Timeout**, an inactivity timer, whose expiration will terminate the tunnel. A value of zero disables the timer. Because tunnels are subject to abrupt termination when the underlying datalink is torn down, use of the Idle Timeout is strongly encouraged.

  An alternate way to force a tunnel to stay up is to define a forced up scheduled connection for the profile.
- Return to the Connection Profile screen by pressing Escape.
- Select **IP Profile Parameters** and press Return. The IP Profile Parameters screen appears.

```
                          IP Profile Parameters

         Address Translation Enabled:       Yes


         NAT Map List...                    Easy-PAT
         NAT Server List...                 Easy-Servers

         Local WAN IP Address:              0.0.0.0

         Remote IP Address:                 173.167.8.10
         Remote IP Mask:                    255.255.0.0

         Filter Set...
         Remove Filter Set

         Receive RIP:                       Both


Enter a subnet mask in decimal and dot form (xxx.xxx.xxx.xxx).
```

- Enter the **Remote IP Address** and **Remote IP Mask** for the host to which you want to tunnel.

Note: A peculiarity associated with VPNs is that when a foreign agent has NAT applied to a Connection Profile set for ATMP data link encapsulation, the home agent and devices behind it, cannot Ping the foreign agent's tunnel end-point IP address. This is because ICMP packets have no port association, and thus will be discarded rather than being processed by NAT.

Ordinarily, Ping is an excellent troubleshooting tool, but it will not be effective in this circumstance. Instead, use another TCP- or UDP-based network service for troubleshooting. Since the Netopia R310 is capable of serving Telnet and HTTP, we recommend using these services instead of Ping.

Allowing VPNs through a Firewall

An administrator interested in securing a network will usually combine the use of VPNs with the use of a firewall or some similar mechanism. This is because a VPN is not a complete security solution, but rather a component of overall security. Using a VPN will add security to transactions carried over a public network, but a VPN alone will not prevent a public network from infiltrating a private network. Therefore, you should combine use of a firewall with VPNs, where the firewall will secure the private network from infiltration from a public network, and the VPN will secure the transactions that must cross the public network.

A strict firewall may not be provisioned to allow VPN traffic to pass back and forth as needed. In order to ensure that a firewall will allow a VPN, certain attributes must be added to the firewall's provisioning. The provisions necessary vary slightly between ATMP and PPTP, but both protocols operate on the same basic premise: there are control and negotiation operations, and there is the tunnelled traffic that carries the payload of data between the VPN endpoints. The difference is that ATMP uses UDP to handle control and negotiation, while PPTP uses TCP. Then both ATMP and PPTP use GRE to carry the payload.

For PPTP negotiation to work, TCP packets inbound and outbound destined for port 1723 must be allowed. Likewise, for ATMP negotiation to work, UDP packets inbound and outbound destined for port 5150 must be allowed. Source ports are dynamic, so, if possible, make this flexible, too. Additionally, PPTP and ATMP both require a firewall to allow GRE bi-directionally.

The following sections illustrate a sample filtering setup to allow either PPTP or ATMP traffic to cross a firewall:

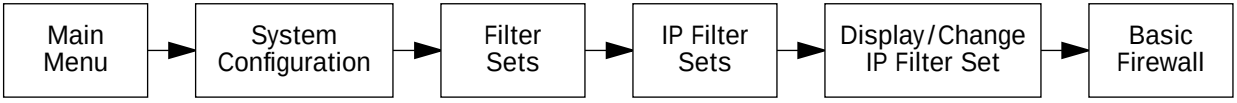
- "PPTP example" on page 10-21
- "ATMP example" on page 10-24

Make your own appropriate substitutions. For more information on filters and firewalls, see Chapter 12, "Security."

PPTP example

To enable a firewall to allow PPTP traffic, you must provision the firewall to allow inbound and outbound TCP packets specifically destined for port 1723. The source port may be dynamic, so often it is not useful to apply a compare function upon this portion of the control/negotiation packets. You must also set the firewall to allow inbound and outbound GRE packets, enabling transport of the tunnel payload.

From the Main Menu navigate to Display/Change IP Filter Set, and from the pop-up menu select **Basic Firewall**.



Select **Display/Change Input Filter**.

Display/Change Input Filter screen

```
+-#----Source IP Addr----Dest IP Addr------Proto-Src.Port-D.Port--On?-Fwd-+
+-------------------------------------------------------------------------+
| 1    0.0.0.0          0.0.0.0           TCP   NC       =1723   Yes Yes |
| 2    0.0.0.0          0.0.0.0           GRE   --       --      Yes Yes |
|                                                                         |
```

For Input Filter 1 set the Destination Port information as shown below.

```
                        Change Input Filter 1

      Enabled:                          Yes
      Forward:                          Yes


      Source IP Address:                0.0.0.0
      Source IP Address Mask:           0.0.0.0

      Dest. IP Address:                 0.0.0.0
      Dest. IP Address Mask:            0.0.0.0

      Protocol Type:                    TCP
      Source Port Compare...            No Compare
      Source Port ID:                   0
      Dest. Port Compare...             Equal
      Dest. Port ID:                    1723
      Established TCP Conns. Only:      No
```

For Input Filter 2 set the Protocol Type to allow GRE as shown below.

```
                        Change Input Filter 2

        Enabled:                            Yes
        Forward:                            Yes


        Source IP Address:                  0.0.0.0
        Source IP Address Mask:             0.0.0.0

        Dest. IP Address:                   0.0.0.0
        Dest. IP Address Mask:              0.0.0.0

        Protocol Type:                      GRE
```

In the Display/Change IP Filter Set screen select **Display/Change Output Filter**.

Display/Change Output Filter screen

```
+-#----Source IP Addr----Dest IP Addr------Proto-Src.Port-D.Port--On?-Fwd-+
+-------------------------------------------------------------------------+
| 1    0.0.0.0          0.0.0.0           TCP   NC       =1723   Yes Yes |
| 2    0.0.0.0          0.0.0.0           GRE   --       --      Yes Yes |
```

For Output Filter 1 set the Protocol Type and Destination Port information as shown below.

```
                        Change Output Filter 1

        Enabled:                            Yes
        Forward:                            Yes


        Source IP Address:                  0.0.0.0
        Source IP Address Mask:             0.0.0.0

        Dest. IP Address:                   0.0.0.0
        Dest. IP Address Mask:              0.0.0.0

        Protocol Type:                      TCP
        Source Port Compare...              No Compare
        Source Port ID:                     0
        Dest. Port Compare...               Equal
        Dest. Port ID:                      1723
        Established TCP Conns. Only:        No
```

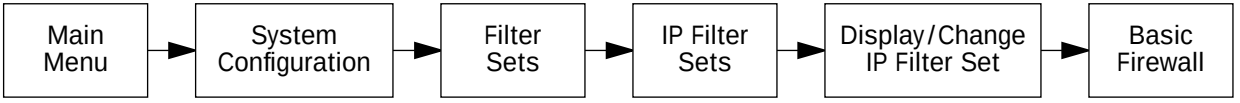
For Output Filter 2 set the Protocol Type to allow GRE as shown below.

```
                    Change Output Filter 2

Enabled:                            Yes
Forward:                            Yes


Source IP Address:                  0.0.0.0
Source IP Address Mask:             0.0.0.0

Dest. IP Address:                   0.0.0.0
Dest. IP Address Mask:              0.0.0.0

Protocol Type:                      GRE
```

ATMP example

To enable a firewall to allow ATMP traffic, you must provision the firewall to allow inbound and outbound UDP packets specifically destined for port 5150. The source port may be dynamic, so often it is not useful to apply a compare function on this portion of the control/negotiation packets. You must also set the firewall to allow inbound and outbound GRE packets (Protocol 47, Internet Assigned Numbers Document, RFC 1700), enabling transport of the tunnel payload.

From the Main Menu navigate to Display/Change IP Filter Set, and from the pop-up menu select **Basic Firewall**.



Select **Display/Change Input Filter**.

Display/Change Input Filter screen

```
+-#----Source IP Addr----Dest IP Addr------Proto-Src.Port-D.Port--On?-Fwd-+
+-------------------------------------------------------------------------+
| 1    0.0.0.0          0.0.0.0          UDP   NC       =5150   Yes Yes |
| 2    0.0.0.0          0.0.0.0          GRE   --       --      Yes Yes |
|                                                                         |
```

For Input Filter 1 set the Destination Port information as shown below.

```
                        Change Input Filter 1

        Enabled:                            Yes
        Forward:                            Yes


        Source IP Address:                  0.0.0.0
        Source IP Address Mask:             0.0.0.0

        Dest. IP Address:                   0.0.0.0
        Dest. IP Address Mask:              0.0.0.0

        Protocol Type:                      TCP
        Source Port Compare...              No Compare
        Source Port ID:                     0
        Dest. Port Compare...               Equal
        Dest. Port ID:                      1723
        Established TCP Conns. Only:        No
```

For Input Filter 2 set the Protocol Type to allow GRE as shown below.

```
                        Change Input Filter 2

        Enabled:                            Yes
        Forward:                            Yes


        Source IP Address:                  0.0.0.0
        Source IP Address Mask:             0.0.0.0

        Dest. IP Address:                   0.0.0.0
        Dest. IP Address Mask:              0.0.0.0

        Protocol Type:                      GRE
```

In the Display/Change IP Filter Set screen select **Display/Change Output Filter**.

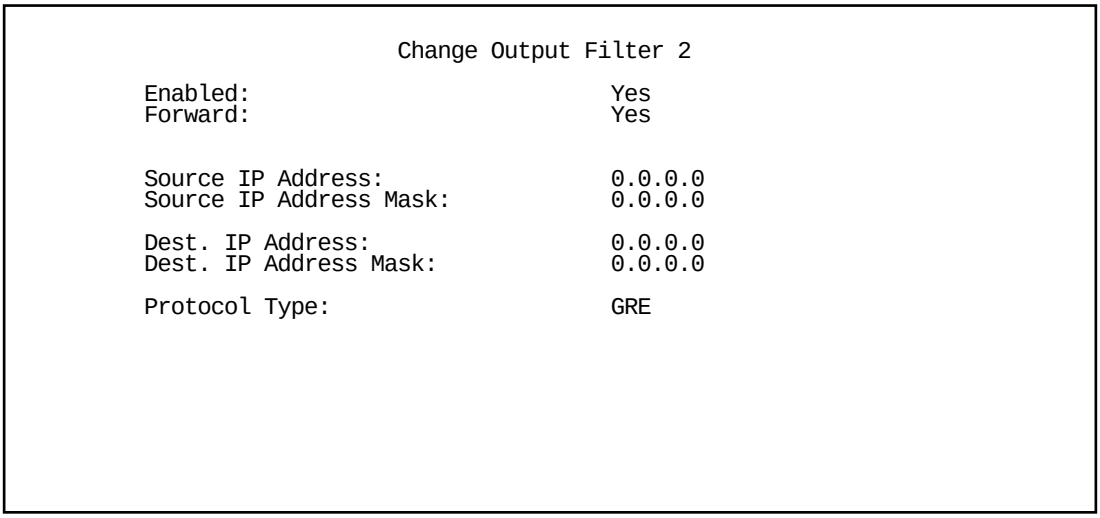
Display/Change Output Filter screen

```
+-#----Source IP Addr----Dest IP Addr------Proto-Src.Port-D.Port--On?-Fwd-+
+-------------------------------------------------------------------------+
| 1    0.0.0.0           0.0.0.0           UDP   NC       NC      Yes Yes |
| 2    0.0.0.0           0.0.0.0           GRE   --       --      Yes Yes |
|                                                                         |
```

For Output Filter 1 set the Protocol Type and Destination Port information as shown below.

```
                        Change Output Filter 1

        Enabled:                            Yes
        Forward:                            Yes


        Source IP Address:                  0.0.0.0
        Source IP Address Mask:             0.0.0.0

        Dest. IP Address:                   0.0.0.0
        Dest. IP Address Mask:              0.0.0.0

        Protocol Type:                      UDP
        Source Port Compare...              No Compare
        Source Port ID:                     0
        Dest. Port Compare...               No Compare
        Dest. Port ID:                      5150
```

For Output Filter 2 set the Protocol Type to allow GRE as shown below.



Chapter 11

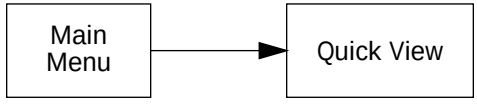
Monitoring Tools

This chapter discusses the Netopia R310's device and network monitoring tools. These tools can provide statistical information, report on current network status, record events, and help in diagnosing and locating problems.

This section covers the following topics:

Quick View status overview

You can get a useful, overall status report from the Netopia R310 in the Quick View screen. To go to the Quick View screen, select **Quick View** in the Main Menu.

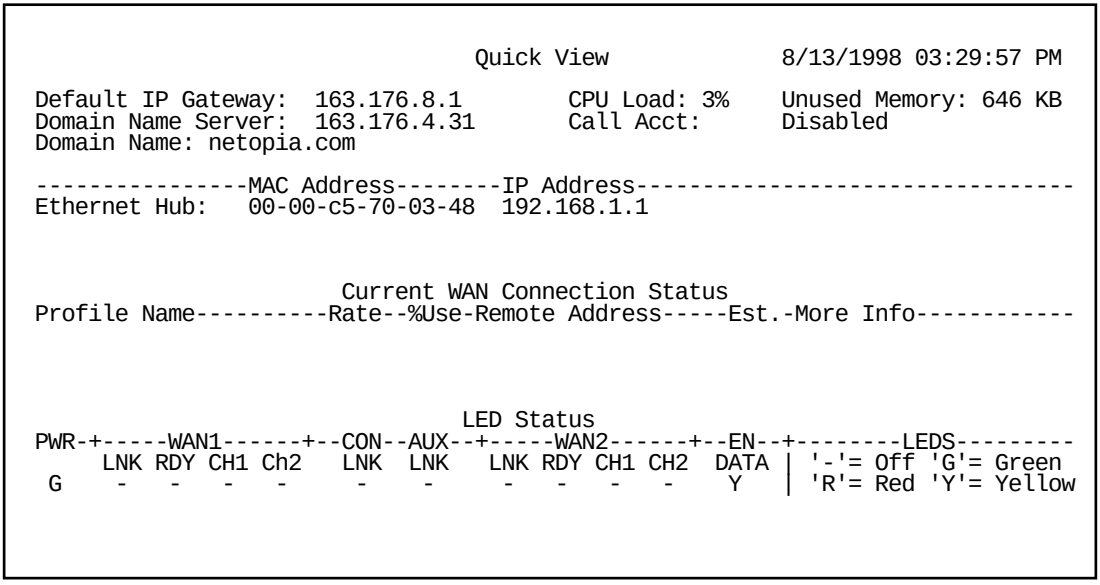


The Quick View screen has three status sections:

- General status
- Current WAN Connection Status
- LED Status

The status sections vary according to the interface of your Netopia R310.

General status



Current Date: The current date; this can be set with the Date and Time utility (see "Date and Time" on page 7-13).

Default IP Gateway: The router's default gateway, which may be either manually configured or learned via DHCP. This is the value you assigned in the Default IP Gateway field on page 6-8. If you are using the router's defaults (DHCP and NAT) this value will be 0.0.0.0. If you have assigned an IP address as your default gateway, it is shown here.

CPU Load: Percentage of the system's resources being used by all current transmissions.

Unused Memory: The total remaining system memory available for use.

Domain Name Server: If you are using the router's defaults (DHCP and NAT) this value will be 0.0.0.0. If you have assigned an IP address as your default gateway, it is shown here.

Call Acct: Shows whether you have enabled or disabled the call accounting features.

Domain Name: the domain name you have assigned, typically the name of your ISP

MAC Address: The Netopia R310's hardware address, for those interfaces that support DHCP.

IP Address: The Netopia R310's IP address, entered in the IP Setup screen.

Current status

The current status section is a table showing the current status of the WAN. For example:

```
                        Current WAN Connection Status
   ---Profile Name------State---%Use-Remote Address----Est.-More Info----------
   ISP                   P1      10  IP 92.163.4.1      Lcl  NAT 192.163.100.6
```

Profile Name: Lists the name of the connection profile being used, if any.

State: Lists the ports in use for this connection.

%Use: Indicates the average percent utilization of the maximum capacity of the channels in use for the connection.

Remote Address: Shows the IP address of the connected remote router if the connection is using IP.

Est: Indicates whether the connection was locally (“Lcl”) or remotely (“Rmt”) established.

More Info: Indicates, in order of priority, the NAT address in use for this connection or the ISDN caller identification (if available).

Status lights

This section shows the current real-time status of the Netopia R310’s status lights (LEDs). It is useful for remotely monitoring the router’s status. The Quick View screen’s arrangement of LEDs corresponds to the physical arrangement of LEDs on the router.

```
-PWR-+-----ISDN------+------------+---------------+--EN--+--------LEDS---------
      LNK RDY CH1 CH2                                DATA  | '-'= Off 'G'= Green
  G    -   G   G   -                                      | 'R'= Red 'Y'= Yellow
```

Each LED representation can report one of four states:

–: A dash means the LED is off.

R: The letter “R” means the LED is red.

G: The letter “G” means the LED is green.

Y: The letter “Y” means the LED is yellow.

The section “Netopia R310 ISDN Router Status Lights” on page 2-4 describes the meanings of the colors for each LED.

Statistics & Logs

When you are troubleshooting your Netopia R310, the Statistics & Logs screens provide insight into the recent event activities of the router.

From the Main Menu go to **Statistics & Logs** and select one of the options described in the sections below.

General Statistics

To go to the General Statistics screen, select **General Statistics** and press Return. The General Statistics screen appears.

```
                              General Statistics

Phys I/F---------Rx Bytes---Tx Bytes---Rx Pkts---Tx Pkts----Rx Err----Tx Err
Ethernet Hub     123456789  123456789  12345678  12345678  12345678  12345678
ISDN B1 Chan     123456789  123456789  12345678  12345678
ISDN B2 Chan     123456789  123456789  12345678  12345678
ISDN D Chan      123456789  123456789  12345678  12345678


Network----------Rx Bytes---Tx Bytes---Rx Pkts---Tx Pkts----Rx Err----Tx Err
IP               123456789  123456789  12345678  12345678  12345678  12345678
```

The General Statistics screen displays information about data traffic on the Netopia R310's data ports. This information is useful for monitoring and troubleshooting your LAN. Note that the counters roll over at their maximum field width, that is, they restart again at 0.

Physical Interface

The top left side of the screen lists total packets received and total packets transmitted for the following data ports:

- Ethernet Hub
- ISDN B1 Channel
- ISDN B2 Channel
- ISDN D Channel

Network Interface

The bottom left side of the screen lists total packets received and total packets transmitted.

The right side of the table lists the total number of occurrences of each of six types of communication statistics:

Rx Bytes. The number of bytes received

Tx Bytes. The number of bytes transmitted

Rx Packets: The number of packets received

Tx Pkts. The number of packets transmitted

Rx Err: The number of bad Ethernet packets received

Tx Err: An error occurring when Ethernet packets are transmitted simultaneously by nodes on the LAN

Event histories

The Netopia R310 records certain relevant occurrences in event histories. Event histories are useful for diagnosing problems because they list what happened before, during, and after a problem occurs. You can view two different event histories: one for the router's system and one for the WAN. The Netopia R310's built-in battery backup prevents loss of event history from a shutdown or reset.

The router's event histories are structured to display the most recent events first, and to make it easy to distinguish error messages from informational messages. Error messages are prefixed with an asterisk. Both the WAN Event History and Device Event History retain records of the 128 most recent events.

In the Statistics & Logs screen, select **WAN Event History**. The WAN Event History screen appears.

WAN Event History

The WAN Event History screen lists a total of 128 events on the WAN. The most recent events appear at the top.

```
                              WAN Event History
                                        Current Date --   9/4/98 01:09:49 PM
 -Date-----Time-----Event-------------------------------------------------------
 ---------------------------------SCROLL UP-------------------------------------
 09/04/98 12:58:34   Link 1 down: Remote clearing, cause: 41, diag: 22
 09/04/98 12:58:34   Issued Clear Response to DN: 5105776430
 09/04/98 12:58:34   Received Clear Ind. from DN: 5105776430, Cause: 41
 09/04/98 12:58:32   Requested Disc. from DN: 5105776431
 09/04/98 12:58:24 >>Issued 64Kb Setup Request from our DN: 5105776430
 09/04/98 10:35:54   Link 2 down: Remote clearing, cause: 41, diag: 50
 09/04/98 10:35:54   Issued Clear Response to DN: 5105776431
 09/04/98 10:35:54   Received Clear Ind. from DN: 5105776431, Cause: 41
 09/04/98 10:35:54   Link 1 down: Remote clearing, cause: 41, diag: 50
 09/04/98 10:35:54   Issued Clear Response to DN: 5105776430
 09/04/98 10:35:54   Received Clear Ind. from DN: 5105776430, Cause: 41
 09/04/98 10:35:44 >>Issued Speech Setup Request from our DN: 5105776431
 09/04/98 10:35:44 >>Issued Speech Setup Request from our DN: 5105776430
 09/04/98 10:35:44 --Device restarted---------------------------------------
 --------------------------------SCROLL DOWN------------------------------------
 Clear History...

Return/Enter on event item for details or SCROLL [UP/DOWN] item for scrolling.
```

Each entry in the list contains the following information:

Time: Time of the event.

Date: Date of the event.

Event: A brief description of the event.

Ch.: The channel involved in the event.

Dir. Number: The directory number (number dialed) involved in the event (switched circuit models only).

The first event in each call sequence is marked with double arrows (>>).

Failures are marked with an asterisk (*).

If the event history exceeds the size of the screen, you can scroll through it by using the SCROLL UP and SCROLL DOWN items.

To scroll up, select **SCROLL UP** at the top of the list and press Return. To scroll down, select **SCROLL DOWN** at the bottom of the list and press Return.

To get more information about any event listed in the WAN Event History, select the event and then press Return. A dialog box containing more information about the selected event will appear. Press Return or Escape to dismiss the dialog box.

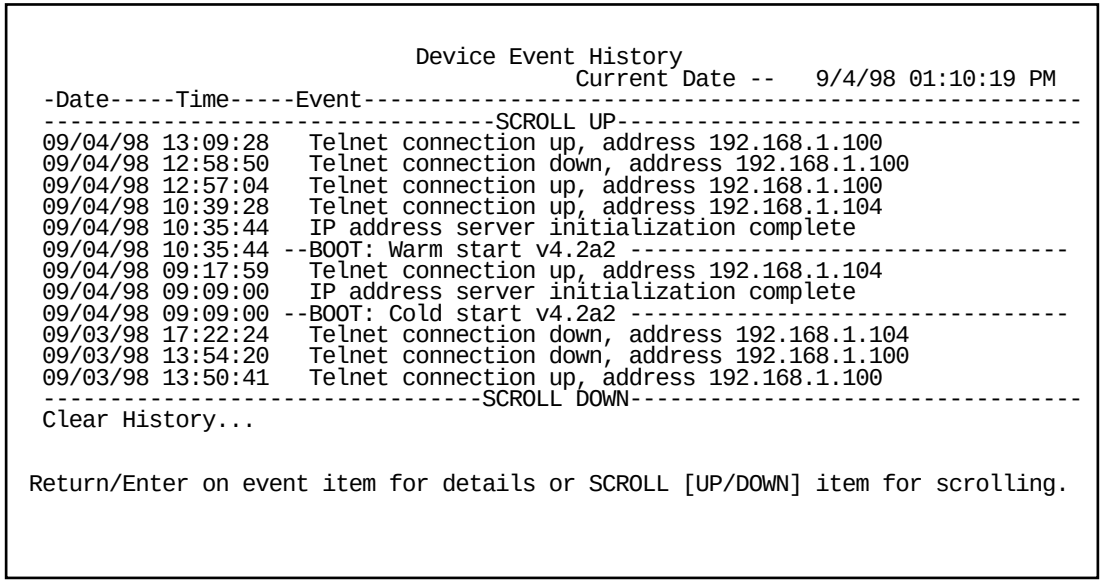
To clear the event history, select **Clear History** at the bottom of the history screen and press Return.

For more information on Event Cause Codes see Appendix F, "Event Histories."

Device Event History

The Device Event History screen lists a total of 128 port and system events, giving the time and date for each event, as well as a brief description. The most recent events appear at the top.

In the Statistics & Logs screen, select **Device Event History**. The Device Event History screen appears.



If the event history exceeds the size of the screen, you can scroll through it by using SCROLL UP and SCROLL DOWN.

To scroll up, select **SCROLL UP** at the top of the list and press Return. To scroll down, select **SCROLL DOWN** at the bottom of the list and press Return.

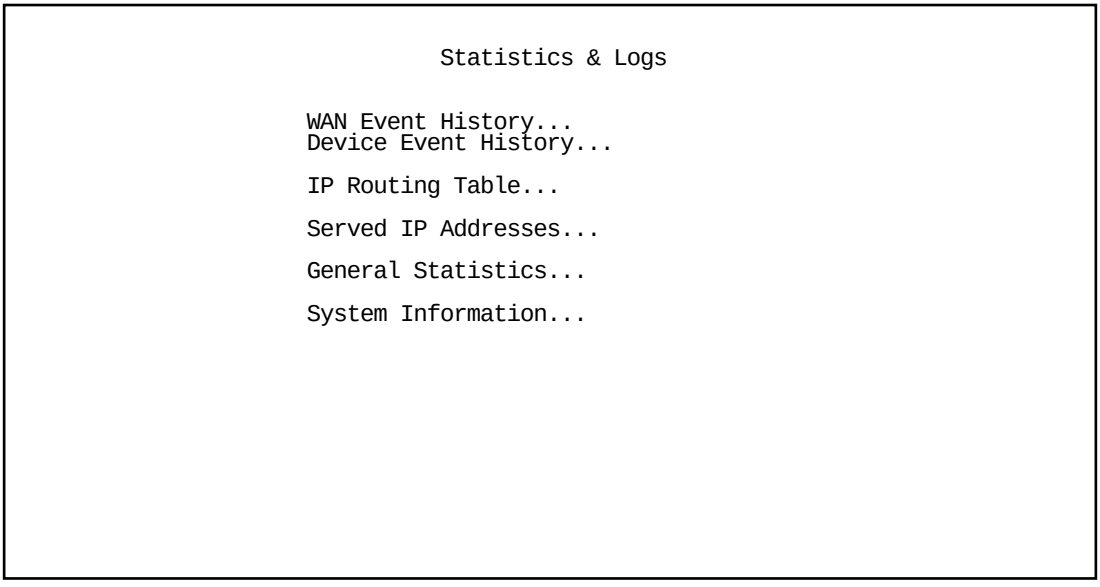
To obtain more information about any event listed in the Device Event History, select the event and then press Return. A dialog box containing more information about the selected event appears. Press Return or Escape to dismiss the dialog box.

To clear the Device Event History, select **Clear History** and press Return.

Routing tables

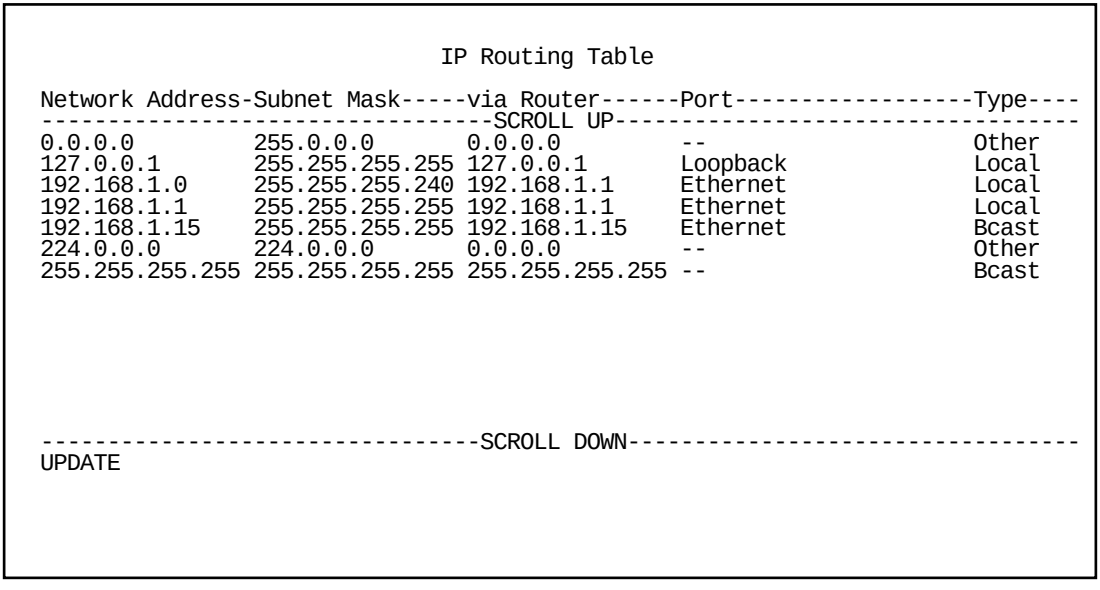
You can view all of the IP routes in the Netopia R310's IP routing tables.

To go to the IP routing table screen, select **IP Routing Table** from the **Statistics & Logs** screen.



The IP routing table displays all of the IP routes currently known to the Netopia R310.

The routing table represents a "snapshot" of the routing table information at the time the screen is first invoked. To take a new snapshot, select **Update** at the bottom of the screen and press Return.



Served IP Addresses

You can view all of the IP addresses currently being served by the Netopia R310 ISDN Router from the **Served IP Addresses** screen.

From the Statistics & Logs menu, select **Served IP Addresses**. The Served IP Addresses screen appears.

```
                          Served IP Addresses

-IP Address-------Type----Expires--Client Identifier--------------------------
---------------------------------SCROLL UP-----------------------------------
 192.168.1.100    DHCP    00:36    EN: 00-00-c5-4a-1f-ea
 192.168.1.101    DHCP    00:58    EN: 08-00-07-16-0c-85
 192.168.1.102
 192.168.1.103
 192.168.1.104
 192.168.1.105
 192.168.1.106
 192.168.1.107
 192.168.1.108
 192.168.1.109
 192.168.1.110
 192.168.1.111
 192.168.1.112
 192.168.1.113
--------------------------------SCROLL DOWN----------------------------------
Lease Management...

  EN = Ethernet Address; CP = Profile Name; HX = hex
```

To manage DHCP leases, select **Lease Management** in this screen.

The IP Address Lease Management screen appears.

```
                      IP Address Lease Management

                          Reset All Leases...

                          Release BootP Leases...

                          Reclaim Declined Addresses...
```

This screen has three options:

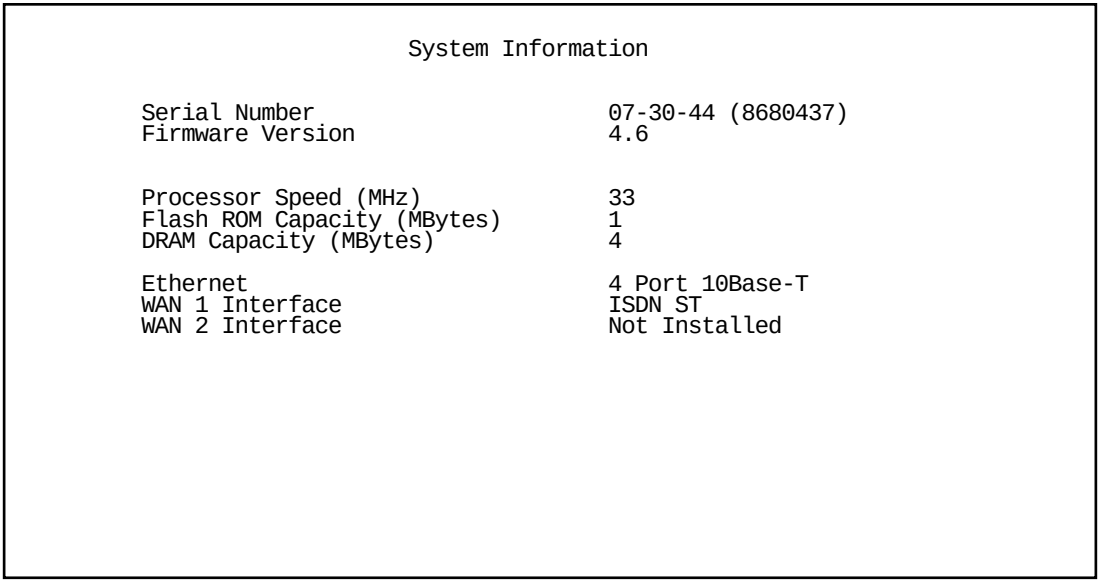
- **Reset All Leases**: Resets all current IP addresses leased through DHCP without waiting for the default one–hour lease period to elapse
- **Release BootP Leases**: Releases any BootP leases that may be in place, and which may no longer be required.

- **Reclaim Declined Addresses**: Reclaims served leases that have been declined; for example by devices that may no longer be on the network.

System Information

The System Information screen gives a summary view of the general system level values in the Netopia R310 ISDN Router.

From the Statistics & Logs menu select **System Information**. The System Information screen appears.



The information display varies by model, firmware version, feature set, and so on. You can tell at a glance your particular system configuration.

SNMP

The Netopia R310 includes a Simple Network Management Protocol (SNMP) agent, allowing monitoring and configuration by a standard SNMP manager.

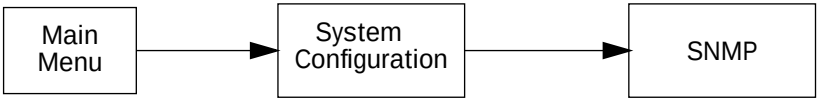
The Netopia R310 supports the following management information base (MIB) documents:

- MIB II (RFC 1213)
- Interface MIB (RFC 1229)
- Ethernet MIB (RFC 1643)
- Netopia MIB

These MIBs are on the Netopia R310 CD included with the Netopia R310. Load these MIBs into your SNMP management software in the order they are listed here. Follow the instructions included with your SNMP manager on how to load MIBs.

The SNMP Setup screen

From the Main Menu, select **SNMP** in the System Configuration screen and press Return. The SNMP Setup screen appears.




```
                                SNMP Setup

          System Name:
          System Location:
          System Contact:


          Read-Only Community String:                  public
          Read/Write Community String:                 private

          Authentication Traps Enable:                 Off

          IP Trap Receivers...




 Configure optional SNMP parameters from here.
```

Follow these steps to configure the first three items in the screen:

1. Select **System Name** and enter a descriptive name for the Netopia R310's SNMP agent.
2. Select **System Location** and enter the router's physical location (room, floor, building, etc.).
3. Select **System Contact** and enter the name of the person responsible for maintaining the router.

System Name, System Location, and System Contact set the values returned by the Netopia R310 SNMP agent for the SysName, SysLocation, and SysContact objects, respectively, in the MIB II system group. Although optional, the information you enter in these items can help a system administrator manage the network more efficiently.

Community strings

The **Read-Only Community String** and the **Read / Write Community String** are like passwords that must be used by an SNMP manager querying or configuring the Netopia R310. An SNMP manager can use the **Read-Only Community String** to examine statistics and configuration information from the router, but will not be able to modify the router's configuration. An SNMP manager can configure and use the **Read / Write Community String** to both examine and modify configuration parameters.

By default, the read-only and read/write community strings are set to "public" and "empty," respectively. You should change the default community strings to values known only to you and trusted system administrators.

To change a community string, select it and enter a new value.

Caution! Even if you decide not to use SNMP, you should change the community strings. This prevents unauthorized access to the Netopia R310 through SNMP. For more information on security issues, see "Suggested security measures" on page 12-1.

SNMP traps

An SNMP **trap** is an informational message sent from an SNMP agent (in this case, the Netopia R310) to a manager. When a manager receives a trap, it may log the trap as well as generate an alert message of its own.

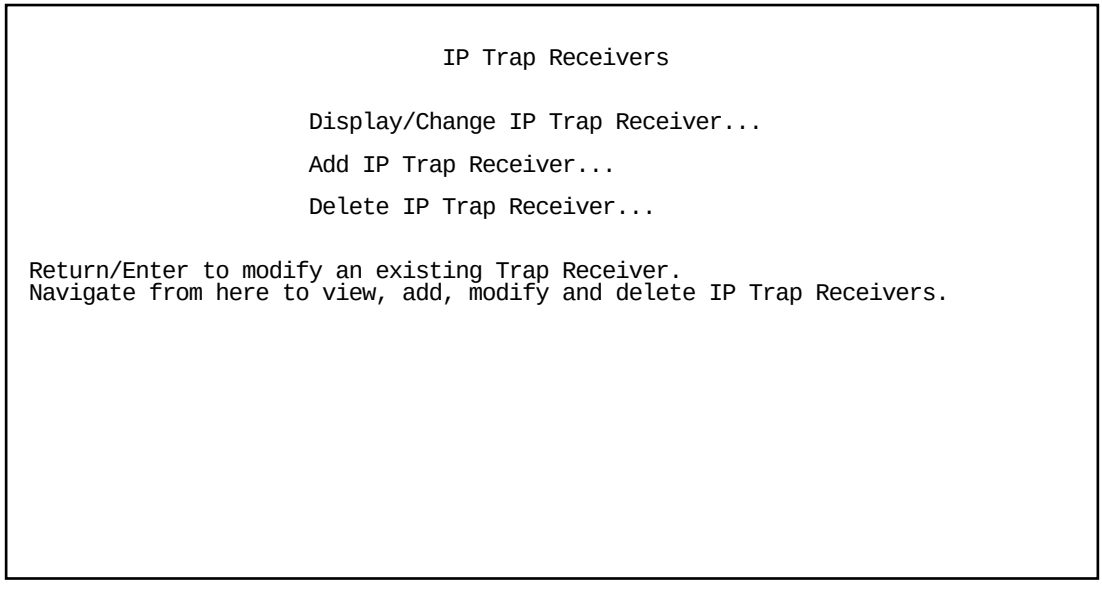
Standard traps generated by the Netopia R310 include the following:

- An authentication failure trap is generated when the router detects an incorrect community string in a received SNMP packet. **Authentication Traps Enable** must be **On** for this trap to be generated.
- A cold start trap is generated after the router is reset.
- An interface down trap (ifDown) is generated when one of the router's interfaces, such as a port, stops functioning or is disabled.
- An interface up trap (ifUp) is generated when one of the router's interfaces, such as a port, begins functioning.

The Netopia R310 sends traps using UDP (for IP networks).

You can specify which SNMP managers are sent the IP traps generated by the Netopia R310. Up to eight receivers can be set. You can also review and remove IP traps.

To go to the IP Trap Receivers screen, select **IP Trap Receivers**. The IP Trap Receivers screen appears.



Setting the IP trap receivers

1. Select **Add IP Trap Receiver**.
2. Select **Receiver IP Address or Domain Name**. Enter the IP address or domain name of the SNMP manager you want to receive the trap.
3. Select **Community String**. Enter whatever community string is appropriate for the traps to be sent to the management station whose IP address or domain name you entered on the previous line.
4. Select **Add Trap Receiver Now** and press Return. You can add up to seven more receivers.

Viewing IP trap receivers

To display a view-only table of IP trap receivers, select **Display / Change IP Trap Receiver** in the IP Trap Receivers screen.

Modifying IP trap receivers

1. To edit an IP trap receiver, select **Display / Change IP Trap Receiver** in the IP Trap Receivers screen.
2. Select an IP trap receiver from the table and press Return.
3. In the **Change IP Trap Receiver** screen, edit the information as needed and press Return.

Deleting IP trap receivers

1. To delete an IP trap receiver, select **Delete IP Trap Receiver** in the IP Trap Receivers screen.
2. Select an IP trap receiver from the table and press Return.
3. In the dialog box, select **Continue** and press Return.

Chapter 12

Security

The Netopia R310 provides a number of security features to help protect its configuration screens and your local network from unauthorized access. Although these features are optional, it is strongly recommended that you use them.

This section covers the following topics:

Suggested security measures

In addition to setting up user accounts, Telnet access, and filters (all of which are covered later in this chapter), there are other actions you can take to make the Netopia R310 and your network more secure:

- Change the SNMP community strings (or passwords). The default community strings are universal and could easily be known to a potential intruder.
- Set the answer profile so it must match incoming calls to a connection profile.
- Use CallerID.
- Leave the "Enable Dial-in Console Access" option set to No.
- Where possible, insist on using PAP, CHAP, or secure authentication token card to authenticate connections to and from connection profiles.
- In high risk areas, configure the Netopia R310 through the serial console port to ensure that your communications cannot be intercepted.

User accounts

When you first set up and configure the Netopia R310, no passwords are required to access the configuration screens. Anyone could tamper with the router's configuration by simply connecting it to a console.

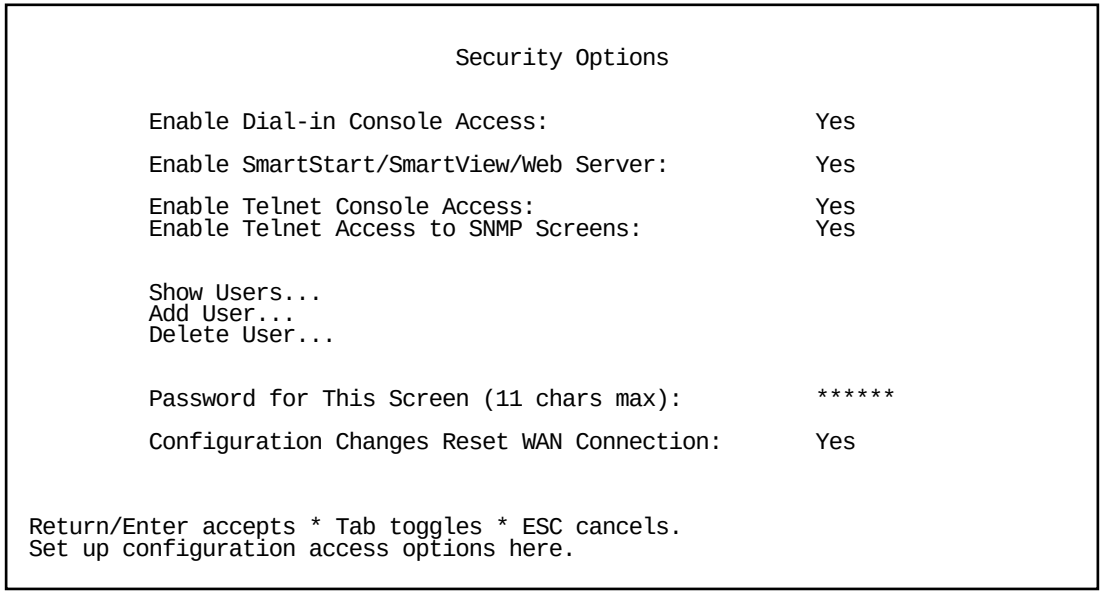
However, by adding user accounts, you can protect the most sensitive screens from unauthorized access. User accounts are composed of name/password combinations that can be given to authorized users.

Caution!

You are strongly encouraged to add protection to the configuration screens. Unprotected screens could allow an unauthorized user to compromise the operation of your entire network.

Once user accounts are created, users who attempt to access protected screens will be challenged. Users who enter an incorrect name or password are returned to a screen requesting a name/password combination to access the Main Menu.

To set up user accounts, select **Security** in the System Configuration screen and go to the Security Options screen.

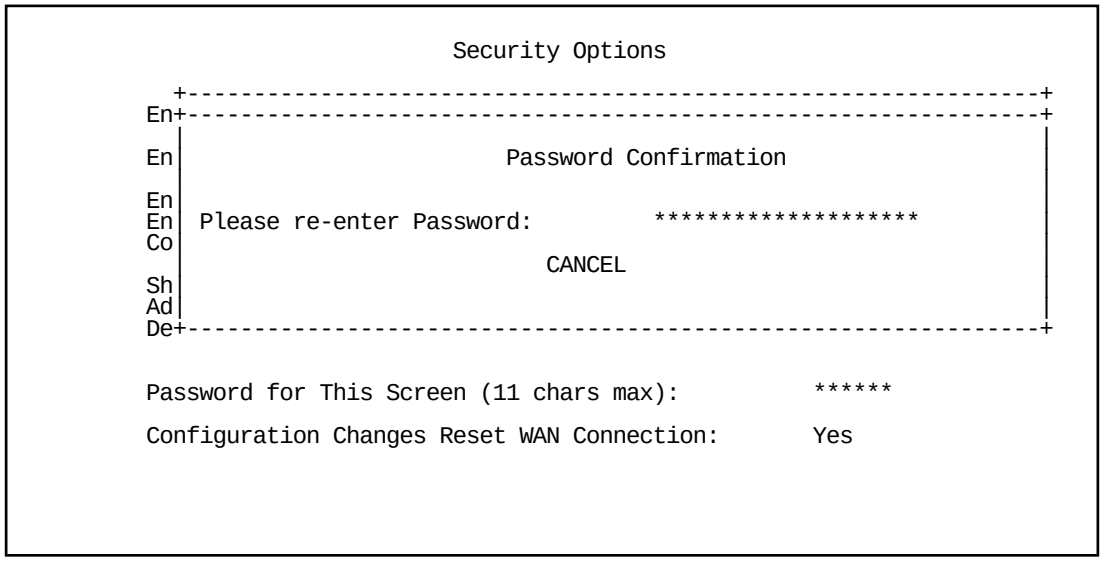


Protecting the Security Options screen

The first screen you should protect is the Security Options screen, because it controls access to the configuration screens. Access to the Security Options screen can be protected with a password.

Select **Password for This Screen** in the Security Options screen and enter a password. The password you enter is displayed as asterisks as shown, rather than clear text. Make sure this password is secure and is different from any of the user account passwords.

When you enter your password, you are prompted to confirm it by re-entering it in a pop-up window.



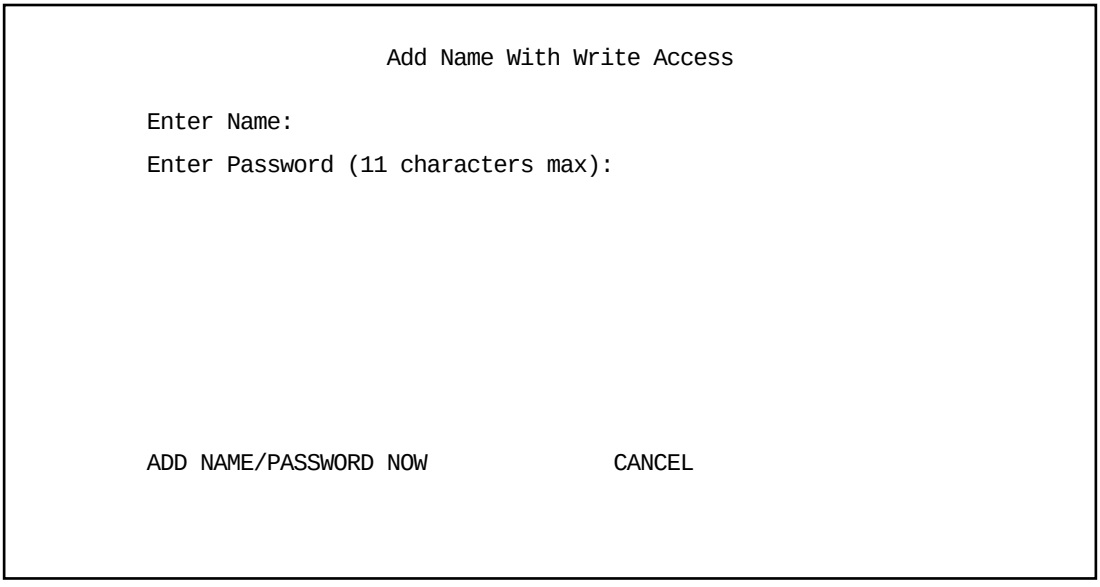
Re-type your password to confirm your entry. When you press **Return**, the password becomes effective.

Protecting the configuration screens

You can protect the configuration screens with user accounts. You can administer the accounts from the Security Options screen. You can create up to four accounts.

To display a view-only list of user accounts, select **Show Users** in the Security Options screen.

To add a new user account, select **Add User** in the Security Options screen and press Return to go to the Add Name With Write Access screen.



Follow these steps to configure the new account:

1. Select **Enter Name** and enter a descriptive name (for example, the user's first name).
2. Select **Enter Password** and enter a password.
3. To accept the new name/password combination, select **ADD NAME/PASSWORD NOW**. To exit the Add Name With Write Access screen without saving the new account, select **CANCEL**.

To delete a user account, select **Delete User** to display a list of accounts. Select an account from the list and press Return to delete it. To exit the list without deleting the selected account, press the Escape key.

Dial-in Console Access

Remote modem terminal emulator setups can dial in to either internal modem line and establish a remote console session, even though they are not using PPP. This allows Netopia Inc.'s "Up and Running, Guaranteed!" department or other administrator with the appropriate security to remotely configure your router for you. If you used SmartStart to configure your router, this option will be set to "No".

- To prevent any remote caller from establishing a remote session, change the option **Enable Dial-in Console Access** to "No".
- To allow access for Up and Running, Guaranteed! with the default name and password in place, toggle this option to "Yes".

Enable SmartStart/SmartView/Web Server

You may wish to restrict access to the web-based screens to prevent inadvertent switching or connecting and disconnecting of Connection Profiles. Since SmartStart can be used to reconfigure the router, you may wish to block inadvertent damage resulting from unauthorized use of SmartStart. To prevent access to these features toggle this option to "No".

Telnet access

Telnet is a TCP/IP service that allows remote terminals to access hosts on an IP network. The Netopia R310 supports Telnet access to its configuration screens.

Caution!

You should consider password-protecting or restricting Telnet access to the Netopia R310 if you suspect there is a chance of tampering.

To password-protect the configuration screens, select Easy Setup from the Main Menu, and go to the **Easy Setup Security Configuration** screen. By entering a Name and Password pair in this screen, all access via serial, Telnet, SNMP, and web server will be password-protected.

To restrict Telnet access, select **Security** in the Advanced Configuration Menu and go to the Security Options screen. There are two levels of Telnet restriction available:

To restrict Telnet access to the SNMP screens, select **Enable Telnet Access to SNMP Screens** and toggle it to **No**. (See "SNMP traps" on page 11-12.)

To restrict Telnet access to all of the configuration screens, select **Enable Telnet Console Access** and toggle it to **No**.

About filters and filter sets

Security should be a high priority for anyone administering a network connected to the Internet. Using packet filters to control network communications can greatly improve your network's security.

The Netopia R310's packet filters are designed to provide security for the Internet connections made to and from your network. You can customize the router's filter sets for a variety of packet filtering applications. Typically, you use filters to selectively admit or refuse TCP/IP connections from certain remote networks and specific hosts. You will also use filters to screen particular types of connections. This is commonly called firewalling your network.

Before creating filter sets, you should read the next few sections to learn more about how these powerful security tools work.

What's a filter and what's a filter set?

A filter is a rule that lets you specify what sort of data can flow in and out of your network. A particular filter can either be an input filter—one that is used on data (packets) coming in to your network from the Internet—or an output filter—one that is used on data (packets) going out from your network to the Internet.

A filter set is a group of filters that work together to check incoming or outgoing data. A filter set can consist of a combination of input and output filters.

How filter sets work

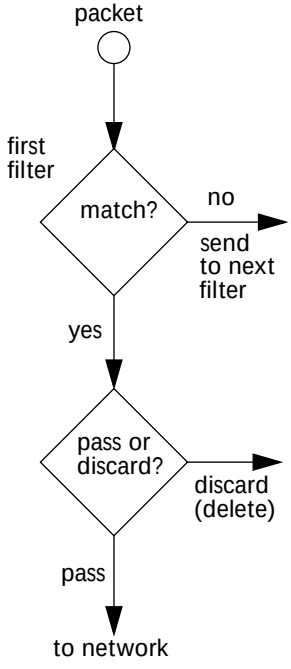
A filter set acts like a team of customs inspectors. Each filter is an inspector through which incoming and outgoing packages must pass. The inspectors work as a team, but each inspects every package individually.

Each inspector has a specific task. One inspector's task may be to examine the destination address of all outgoing packages. That inspector looks for a certain destination—which could be as specific as a street address or as broad as an entire country—and checks each package's destination address to see if it matches that destination.

A filter inspects data packets like a customs inspector scrutinizing packages.

Filter priority

Continuing the customs inspectors analogy, imagine the inspectors lined up to examine a package. If the package matches the first inspector's criteria, the package is either rejected or passed on to its destination, depending on the first inspector's particular orders. In this case, the package is never seen by the remaining inspectors.



If the package does not match the first inspector's criteria, it goes to the second inspector, and so on. You can see that the order of the inspectors in the line is very important.

For example, let's say the first inspector's orders are to send along all packages that come from Rome, and the second inspector's orders are to reject all packages that come from France. If a package arrives from Rome, the first inspector sends it along without allowing the second inspector to see it. A package from Paris is ignored by the first inspector, rejected by the second inspector, and never seen by the others. A package from London is ignored by the first two inspectors, and so it's seen by the third inspector.

In the same way, filter sets apply their filters in a particular order. The first filter applied can pass or discard a packet before that packet ever reaches any of the other filters. If the first filter can neither pass nor discard the packet (because it cannot match any criteria), the second filter has a chance to pass or reject it, and so on. Because of this hierarchical structure, each filter is said to have a priority. The first filter has the highest priority, and the last filter has the lowest priority.

How individual filters work

As described above, a filter applies criteria to an IP packet and then takes one of three actions:

A filter's actions

- Passes the packet to the local or remote network
- Blocks (discards) the packet
- Ignores the packet

A filter passes or blocks a packet only if it finds a match after applying its criteria. When no match occurs, the filter ignores the packet.

The criteria are based on information contained in the packets. A filter is simply a rule that prescribes certain actions based on certain conditions. For example, the following rule qualifies as a filter:

A filtering rule

Block all Telnet attempts that originate from the remote host 199.211.211.17.

This rule applies to Telnet packets that come from a host with the IP address 199.211.211.17. If a match occurs, the packet is blocked.

Here is what this rule looks like when implemented as a filter on the Netopia R310:

```
+-#--Source IP Addr--Dest IP Addr-----Proto-Src.Port-D.Port--On?-Fwd-+
+-------------------------------------------------------------------+
| 1  199.211.211.17  0.0.0.0          TCP      0      23     Yes No  |
+-------------------------------------------------------------------+
```

To understand this particular filter, look at the parts of a filter.

Parts of a filter

A filter consists of criteria based on packet attributes. A typical filter can match a packet on any one of the following attributes:

- The source IP address (where the packet was sent from)
- The destination IP address (where the packet is going)
- The type of higher-layer Internet protocol the packet is carrying, such as TCP or UDP

Port numbers

A filter can also match a packet's port number attributes, but only if the filter's protocol type is set to TCP or UDP, since only those protocols use port numbers. The filter can be configured to match the following:

- The source port number (the port on the sending host that originated the packet)
- The destination port number (the port on the receiving host that the packet is destined for)

By matching on a port number, a filter can be applied to selected TCP or UDP services, such as Telnet, FTP, and World Wide Web. The tables below show a few common services and their associated port numbers..

Internet service	TCP port	Internet service	TCP port
FTP	20/21	Finger	79
Telnet	23	World Wide Web	80
SMTP (mail)	25	News	144
Gopher	70	rlogin	513

Internet service	UDP port	Internet service	UDP port
Who Is	43	TFTP	69
World Wide Web	80	who	513
SNMP	161		

Port number comparisons

A filter can also use a comparison option to evaluate a packet's source or destination port number. The comparison options are:

No Compare: No comparison of the port number specified in the filter with the packet's port number.

Not Equal To: For the filter to match, the packet's port number cannot equal the port number specified in the filter.

Less Than: For the filter to match, the packet's port number must be less than the port number specified in the filter.

Less Than or Equal: For the filter to match, the packet's port number must be less than or equal to the port number specified in the filter.

Equal: For the filter to match, the packet's port number must equal the port number specified in the filter.

Greater Than: For the filter to match, the packet's port number must be greater than the port number specified in the filter.

Greater Than or Equal: For the filter to match, the packet's port number must be greater than or equal to the port number specified in the filter.

Other filter attributes

There are three other attributes to each filter:

- The filter's order (i.e., priority) in the filter set
- Whether the filter is currently active
- Whether the filter is set to pass (forward) packets or to block (discard) packets

Putting the parts together

When you display a filter set, its filters are displayed as rows in a table:

```
+-#---Source IP Addr---Dest IP Addr-----Proto-Src.Port-D.Port--On?-Fwd-+
+-------------------------------------------------------------------+
| 1   192.211.211.17   0.0.0.0          TCP   0        23      Yes No  |
| 2   0.0.0.0          0.0.0.0          TCP   NC       =6000   Yes No  |
| 3   0.0.0.0          0.0.0.0          ICMP  --       --      Yes Yes |
| 4   0.0.0.0          0.0.0.0          TCP   NC       >1023   Yes Yes |
| 5   0.0.0.0          0.0.0.0          UDP   NC       >1023   Yes Yes |
|                                                                   |
|                                                                   |
|                                                                   |
|                                                                   |
|                                                                   |
|                                                                   |
|                                                                   |
|                                                                   |
+-------------------------------------------------------------------+
```

The table's columns correspond to each filter's attributes:

#: The filter's priority in the set. Filter number 1, with the highest priority, is first in the table.

Source IP Addr: The packet source IP address to match.

Dest IP Addr: The packet destination IP address to match.

Proto: The protocol to match. This can be entered as a number (see the table below) or as TCP or UDP if using those protocols.

Protocol	Number to use	Full name
N/A	0	Ignores protocol type
ICMP	1	Internet Control Message Protocol
TCP	6	Transmission Control Protocol
UDP	17	User Datagram Protocol

Src. Port: The source port to match. This is the port on the sending host that originated the packet.

D. Port: The destination port to match. This is the port on the receiving host for which the packet is intended.

On?: Displays **Yes** when the filter is in effect or **No** when it is not.

Fwd: Shows whether the filter forwards (**Yes**) a packet or discards (**No**) it when there's a match.

Filtering example #1

Returning to our filtering rule example from above (see page 12-7), look at how a rule is translated into a filter. Start with the rule, then fill in the filter's attributes:

1. The rule you want to implement as a filter is:

   Block all Telnet attempts that originate from the remote host 199.211.211.17.

2. The host 199.211.211.17 is the source of the Telnet packets you want to block, while the destination address is any IP address. How these IP addresses are masked determines what the final match will be, although the mask is not displayed in the table that displays the filter sets (you set it when you create the filter). In fact, since the mask for the destination IP address is 0.0.0.0, the address for Dest IP Addr could have been anything. The mask for Source IP Addr must be 255.255.255.255 since an exact match is desired.

   - Source IP Addr = 199.211.211.17
   - Source IP address mask = 255.255.255.255
   - Dest IP Addr = 0.0.0.0
   - Destination IP address mask = 0.0.0.0

   Note: To learn about IP addresses and masks, see Appendix D, "Understanding IP Addressing."

3. Using the tables on page 12-8, find the destination port and protocol numbers (the *local* Telnet port):

   - Proto = TCP (or 6)
   - D. Port = 23

4. The filter should be enabled and instructed to block the Telnet packets containing the source address shown in step 2:
   - On? = Yes
   - Fwd = No

This four-step process is how we produced the following filter from the original rule:

```
+-#---Source IP Addr---Dest IP Addr-----Proto-Src.Port-D.Port--On?-Fwd-+
+-------------------------------------------------------------------------+
| 1   192.211.211.17   0.0.0.0          TCP   0        23      Yes No   |
|                                                                         |
+-------------------------------------------------------------------------+
```

Filtering example #2

Suppose a filter is configured to block all incoming IP packets with the source IP address of 200.233.14.0, regardless of the type of connection or its destination. The filter would look like this:

```
+-#---Source IP Addr---Dest IP Addr-----Proto-Src.Port-D.Port--On?-Fwd-+
+-------------------------------------------------------------------------+
| 1   200.233.14.0     0.0.0.0               0               Yes No   |
|                                                                         |
+-------------------------------------------------------------------------+
```

This filter blocks any packets coming from a remote network with the IP network address 200.233.14.0. The 0 at the end of the address signifies *any* host on the class C IP network 200.233.14.0. If, for example, the filter is applied to a packet with the source IP address 200.233.14.5, it will block it.

In this case, the mask, which does not appear in the table, must be set to 255.255.255.0. This way, all packets with a source address of 200.233.14.x will be matched correctly, no matter what the final address byte is.

Note: The protocol attribute for this filter is 0 by default. This tells the filter to ignore the IP protocol or type of IP packet.

Design guidelines

Careful thought should go into designing a new filter set. You should consider the following guidelines:

- Be sure the filter set's overall purpose is clear from the beginning. A vague purpose can lead to a faulty set, and that can actually make your network *less* secure.
- Be sure each individual filter's purpose is clear.
- Determine how filter priority will affect the set's actions. Test the set (on paper) by determining how the filters would respond to a number of different hypothetical packets.
- Consider the combined effect of the filters. If every filter in a set fails to match on a particular packet, the packet is:
  - passed if all the filters are configured to discard (*not* forward).

- discarded if all the filters are configured to pass (forward).
- discarded if the set contains a combination of pass and discard filters.

Disadvantages of filters

Although using filter sets can greatly enhance network security, there are disadvantages:

- Filters are complex. Combining them in filter sets introduces subtle interactions, increasing the likelihood of implementation errors.
- Enabling a large number of filters can have a negative impact on performance. Processing of packets will take longer if they have to go through many checkpoints.
- Too much reliance on packet filters can cause too little reliance on other security methods. Filter sets are *not* a substitute for password protection, effective safeguarding of passwords, caller ID, the "must match" option in the answer profile, PAP or CHAP in connection profiles, callback, and general awareness of how your network may be vulnerable.

An approach to using filters

The ultimate goal of network security is to prevent unauthorized access to the network without compromising authorized access. Using filter sets is part of reaching that goal.

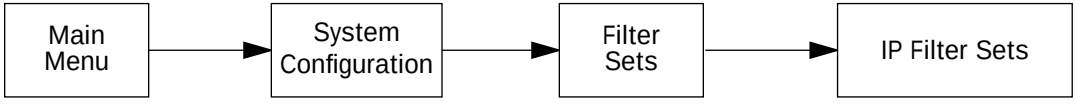
Each filter set you design will be based on one of the following approaches:

- That which is not expressly prohibited is permitted.
- That which is not expressly permitted is prohibited.

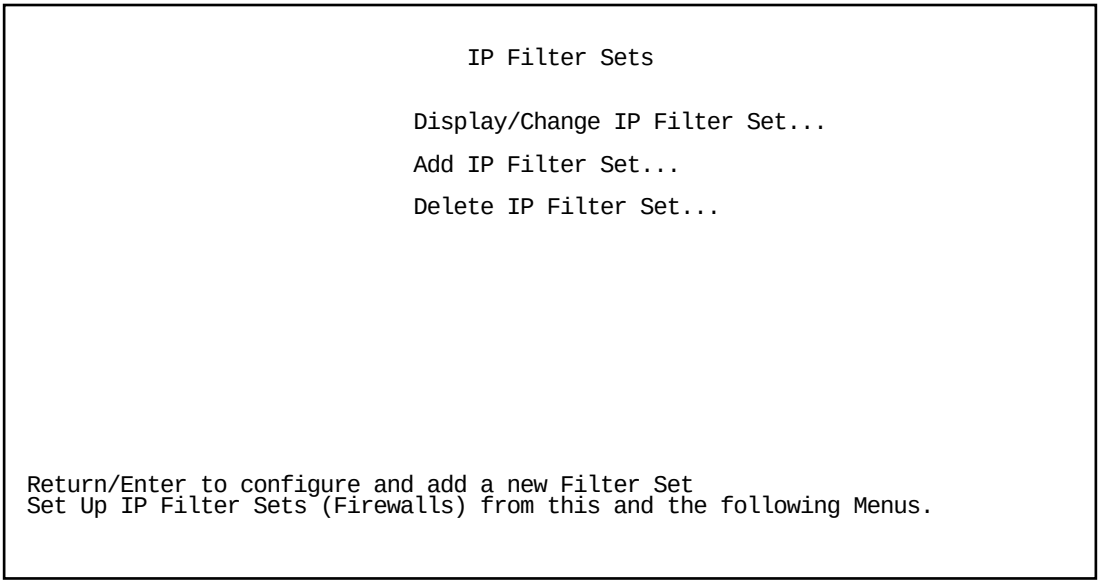
It is strongly recommended that you take the latter, and safer, approach to all of your filter set designs.

Working with IP filters and filter sets

To work with filters and filter sets, begin by accessing the filter set screens.



Note: Make sure you understand how filters work before attempting to use them. Read the section "About filters and filter sets," beginning on page 12-5.



The procedure for creating and maintaining filter sets is as follows:

1. Add a new filter set.
2. Create the filters for the new filter set.
3. View, change, or delete individual filters and filter sets.

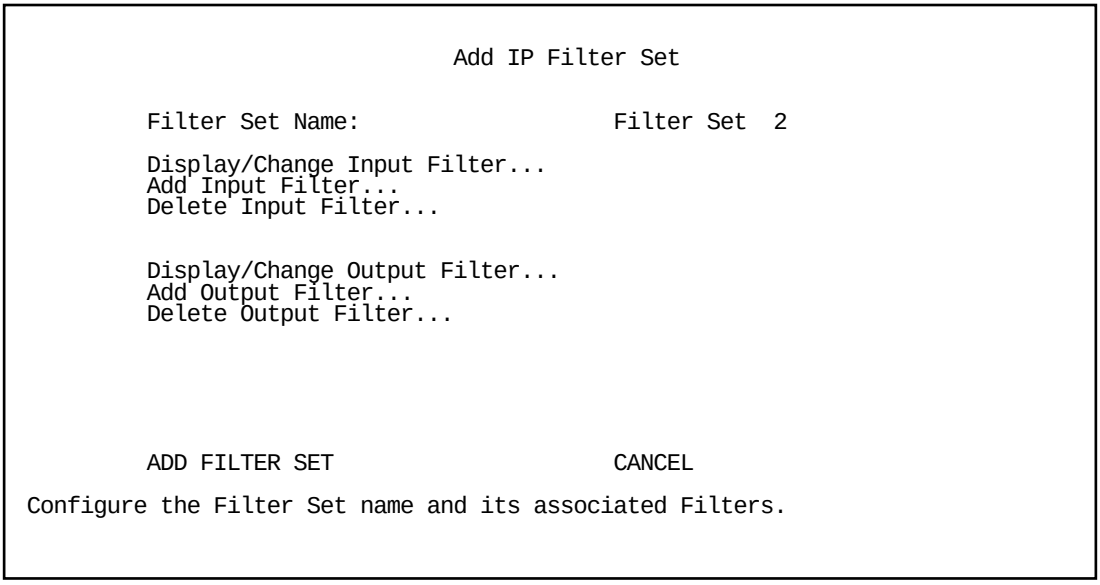
The sections below explain how to execute these steps.

Adding a filter set

You can create up to eight different custom filter sets. Each filter set can contain up to 255 filter rules, in any combination of input or output.

To add a new filter set, select **Add IP Filter Set** in the IP Filter Sets screen and press Return to go to the Add Filter Set screen.

Note: There are two groups of items in the Add Filter Set screen, one for input filters and one for output filters. The two groups work in essentially the same way, as you'll see below.



Naming a new filter set

All new filter sets have a default name. The first filter set you add will be called Filter Set 1, the next filter will be Filter Set 2, and so on.

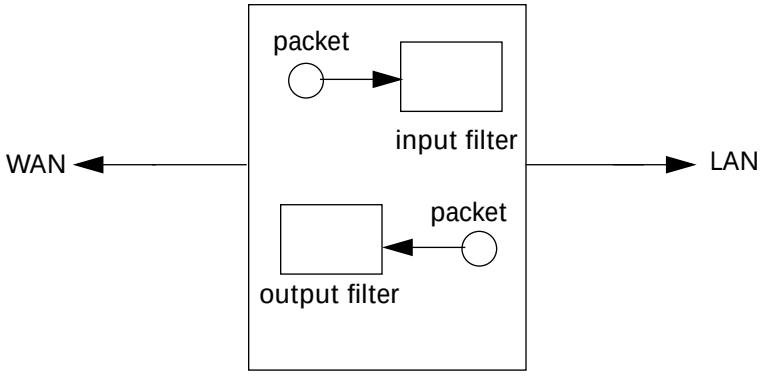
To give a new filter set a different name, select **Filter Set Name** and enter a new name for the filter set.

To save the filter set, select **ADD FILTER SET**. The saved filter set is empty (contains no filters), but you can return to it later to add filters (see "Modifying filter sets" on page 12-18). Or you can add filters to your new set before saving it (see "Adding filters to a filter set" on page 12-15).

Select **CANCEL** to leave the Add Filter Set screen without saving the new filter set and return to the Filter Sets screen.

Input and output filters—source and destination

There are two kinds of filters you can add to a filter set: input and output. Input filters check packets received from the Internet, destined for your network. Output filters check packets transmitted from your network to the Internet. You might use output filters, for example to selectively control which users on your network have access to the Internet or to a remote corporate network.



Packets in the Netopia R310 pass through an input filter if they originate in the WAN and through an output filter if they're being sent out to the WAN.

The process for adding input and output filters is exactly the same. The main difference between the two involves their reference to **source** and **destination**. From the perspective of an input filter, your local network is the **destination** of the packets it checks, and the remote network is their **source**. From the perspective of an output filter, your local network is the **source** of the packets, and the remote network is their **destination**.

Type of filter	"source" means	"destination" means
Input filter	the remote network	the local network
Output filter	the local network	the remote network

Adding filters to a filter set

In this section you'll learn how to add an input filter to a filter set. Adding an output filter works exactly the same way, providing you keep the different source and destination perspectives in mind.

To add an input filter, select **Add Input Filter** in the Add IP Filter Set screen and go to the Add Filter screen. (Select **Add Output Filter** to add an output filter.)

```
                              Add Input Filter

          Enabled:                            Yes
          Forward:                            No


          Source IP Address:                  0.0.0.0
          Source IP Address Mask:             0.0.0.0

          Dest. IP Address:                   0.0.0.0
          Dest. IP Address Mask:              0.0.0.0

          Protocol Type:                      ICMP
          ICMP Type Compare...                Equal
          ICMP Type:                          0
          ICMP Code Compare...                No Compare
          ICMP Code:                          0


          ADD THIS FILTER NOW                 CANCEL

Enter a type: 'ICMP', 'UDP', 'TCP', 'Any', or a number between 0 and 255.
```

1. To make the filter active in the filter set, select **Enabled** and toggle it to **Yes**. If **Enabled** is toggled to **No**, the filter can still exist in the filter set, but it will have no effect.
2. If you want the filter to forward packets that match its criteria to the destination IP address, select **Forward** and toggle it to **Yes**. If **Forward** is toggled to **No**, packets matching the filter's criteria will be discarded.
3. Select **Source IP Address** and enter the source IP address this filter will match on. You can enter a subnet or a host address.
4. Select **Source IP Address Mask** and enter a mask for the source IP address. This allows you to further modify the way the filter will match on the source address. Enter 0.0.0.0 to force the filter to match on all source IP addresses, or enter 255.255.255.255 to match the source IP address exclusively.
5. Select **Dest. IP Address** and enter the destination IP address this filter will match on. You can enter a subnet or a host address.
6. Select **Dest. IP Address Mask** and enter a mask for the destination IP address. This allows you to further modify the way the filter will match on the destination address. Enter 0.0.0.0 to force the filter to match on all destination IP addresses.
7. Select **Protocol Type** and enter **ICMP**, **TCP**, **UDP**, **Any**, or the number of another IP transport protocol (see the table on page 12-10).

   Note: If you enter **ICMP** or **1**, the **ICMP Type Compare** and **ICMP Code Compare** fields display. See steps 8., 10., 9., and 11. below.

   If you enter **TCP** or **UDP**, the **Source Port Compare**, **Source Port ID,** and **Dest. Port Compare** fields display. See steps 12. and 13. below.
8. If the Protocol Type is ICMP, select **ICMP Type Compare** and choose one of the following options from the pop-up menu: No Compare, Not Equal To, Less Than, Less Than or Equal, Equal, Greater Than or Equal, or Greater Than.
9. Every ICMP packet has an 8-bit integer field, *Type*, that identifies what kind of ICMP packet (of 13 possible packet types) it is. Select **ICMP Types** and select the packet type. The choices are:

Type	Description
0	Echo reply
3	Destination unreachable
8	Echo request

10. Select **ICMP Code Compare** and choose one of the following options from the pop-up menu: No Compare, Not Equal To, Less Than, Less Than or Equal, Equal, Greater Than or Equal, or Greater Than.
11. In addition to the Type, an 8-bit field, *Code*, gives more information about the Type. Select **ICMP Codes** and select more information about the type. The choices are:

Code	Description
0	Network Unreachable
1	Host unreachable
6	Destination network unknown
7	Destination host unknown

    It is unlikely that you would need to filter on ICMP code types. However, if you should find it necessary, refer to standard texts on internetworking with TCP/IP for more information.

    Now skip to step 14.

12. If the **Protocol Type** is **TCP** or **UDP**, select **Source Port Compare** and choose a comparison method for the filter to use on a packet's source port number. Then select **Source Port ID** and enter the actual source port number to match on (see the table on page 12-8).

    Note: If the **Protocol Type** is **ICMP**, you will not see this field.

13. Select **Dest. Port Compare** and choose a comparison method for the filter to use on a packet's destination port number. Then select **Dest. Port ID** and enter the actual destination port number to match on (see the table on page 12-8).

    Note: If the **Protocol Type** is **ICMP**, you will not see this field.

14. When you are finished configuring the filter, select **ADD THIS FILTER NOW** to save the filter in the filter set. Select **CANCEL** to discard the filter.

Viewing filters

To display a view-only table of input (output) filters, select **Display/Change Input Filters** (**Display/Change Output Filters**) in the Add IP Filter Set screen.

Modifying filters

To modify a filter, select **Display / Change Input Filter** (**Display / Change Output Filter**) in the Add IP Filter Set screen to display a table of filters.

Select a filter from the table and press Return to go to the Change Filter screen. The parameters in this screen are the same as the ones in the Add Filter screen (see "Adding filters to a filter set" on page 12-15).

```
                                  Change Filter

                        Enabled:                    No
                        Forward:                    No

                        Source IP Address:          0.0.0.0
                        Source IP Address Mask:     0.0.0.0

                        Dest. IP Address:           0.0.0.0
                        Dest. IP Address Mask:      0.0.0.0

                        Protocol Type:              0

                        Source Port Compare...      No Compare
                        Source Port ID:             0
                        Dest. Port Compare...       No Compare
                        Dest. Port ID:              0


Enter the IP specific information for this filter.
```

Deleting filters

To delete a filter, select **Delete Input Filter** (**Delete Output Filter**) in the Add Filter Set screen to display a table of filters.

Select the filter from the table and press Return to delete it. Press the Escape key to exit the table without deleting the filter.

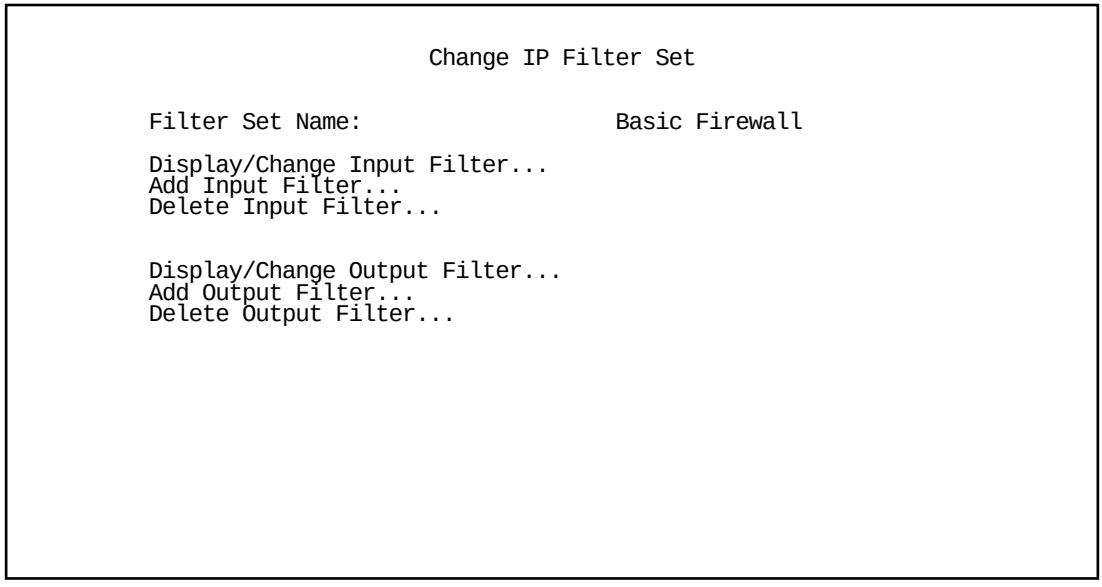
Viewing filter sets

To display a view-only list of filter sets, select **Display / Change Filter Sets** in the IP Filter Sets screen.

Modifying filter sets

To modify a filter set, select **Display / Change Filter Set** in the Filter Sets screen to display a list of filter sets.

Select a filter set from the list and press Return to go to the Change IP Filter Set screen. The items in this screen are the same as the ones in the Add Filter screen (see "Adding filters to a filter set" on page 12-15).



Deleting a filter set

Note: If you delete a filter set, all of the filters it contains are deleted as well. To reuse any of these filters in another set, you'll have to note their configuration before deleting the current filter set and then recreate them.

To delete a filter set, select **Delete Filter Set** in the IP Filter Sets screen to display a list of filter sets.

Select a filter set from the list and press Return to delete it. Press the Escape key to exit the list without deleting the filter set.

A sample IP filter set

This section contains the settings for a filter set, called Basic Firewall, which is part of the Netopia R310's factory configuration.

Basic Firewall blocks undesirable traffic originating from the WAN (in most cases, the Internet), but passes all traffic originating from the LAN. It follows the conservative "that which is not expressly permitted is prohibited" approach: unless an incoming packet expressly matches one of the constituent input filters, it will not be forwarded to the LAN.

The five input filters and one output filter that make up Basic Firewall are shown in the table below.

Setting	Input filter 1	Input filter 2	Input filter 3	Input filter 4	Input filter 5	Output filter 1
Enabled	Yes	Yes	Yes	Yes	Yes	Yes
Forward	No	No	Yes	Yes	Yes	Yes
Source IP address	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
Source IP address mask	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
Dest. IP address	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
Dest. IP address mask	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
Protocol type	TCP	TCP	ICMP	TCP	UDP	0
Source port comparison	No Compare	No Compare	N/A	No Compare	No Compare	N/A
Source port ID	0	0	N/A	0	0	N/A
Dest. port comparison	Equal	Equal	N/A	Greater Than	Greater Than	N/A
Dest. port ID	2000	6000	N/A	1023	1023	N/A

Basic Firewall's filters play the following roles.

Input filters 1 and 2: These block WAN-originated OpenWindows and X-Windows sessions. Service origination requests for these protocols use ports 2000 and 6000, respectively. Since these are greater than 1023, OpenWindows and X-Windows traffic would otherwise be allowed by input filter 4. Input filters 1 and 2 must precede input filter 4; otherwise they would have no effect as filter 4 would have already passed OpenWindows and X-Windows traffic.

Input filter 3: This filter explicitly passes all WAN-originated ICMP traffic to permit devices on the WAN to ping devices on the LAN. Ping is an Internet service that is useful for diagnostic purposes.

Input filters 4 and 5: These filters pass all TCP and UDP traffic, respectively, when the destination port is greater than 1023. This type of traffic generally does not allow a remote host to connect to the LAN using one of the potentially intrusive Internet services, such as Telnet, FTP, and WWW.

Output filter 1: This filter passes all outgoing traffic to make sure that no outgoing connections from the LAN are blocked.

Basic Firewall is suitable for a LAN containing only client hosts that wish to access servers on the WAN, not for a LAN containing servers providing services to clients on the WAN. Basic Firewall's general strategy is to explicitly pass WAN-originated TCP and UDP traffic to ports greater than 1023. Ports lower than 1024 are the service origination ports for various Internet services such as FTP, Telnet, and the World Wide Web (WWW).

A more complicated filter set would be required to provide WAN access to a LAN-based server. See "Possible modifications," below, for ways to allow remote hosts to use services provided by servers on the LAN.

Possible modifications

You can modify the sample filter set Basic Firewall to allow incoming traffic using the examples below. These modifications are not intended to be combined. Each modification is to be the only one used with Basic Firewall.

The results of combining filter set modifications can be difficult to predict. It is recommended that you take special care if making more than one modification to the sample filter set.

Trusted host. To allow unlimited access by a trusted remote host with the IP address a.b.c.d (corresponding to a numbered IP address such as 163.176.8.243), insert the following input filter ahead of the current input filter 1:

- Enabled: Yes
- Forward: Yes
- Source IP Address: a.b.c.d
- Source IP Address Mask: 255.255.255.255
- Dest. IP Address: 0.0.0.0
- Dest. IP Address Mask: 0.0.0.0
- Protocol Type: 0

Trusted subnet. To allow unlimited access by a trusted remote subnet with subnet address a.b.c.d (corresponding to a numbered IP address such as 163.176.8.0) and subnet mask e.f.g.h (corresponding to a numbered IP mask such as 255.255.255.0), insert the following input filter ahead of the current input filter 1:

- Enabled: Yes
- Forward: Yes
- Source IP Address: a.b.c.d
- Source IP Address Mask: e.f.g.h
- Dest. IP Address: 0.0.0.0
- Dest. IP Address Mask: 0.0.0.0
- Protocol Type: 0

FTP sessions. To allow WAN-originated FTP sessions to a LAN-based FTP server with the IP address a.b.c.d (corresponding to a numbered IP address such as 163.176.8.243), insert the following input filter ahead of the current input filter 1:

- Enabled: Yes
- Forward: Yes
- Source IP Address: 0.0.0.0
- Source IP Address Mask: 0.0.0.0
- Dest. IP Address: a.b.c.d
- Dest. IP Address Mask: 255.255.255.255
- Protocol Type: TCP
- Source Port Comparison: No Compare
- Source Port ID: 0
- Dest. Port Comparison: Equal
- Dest. Port ID: 21

Note: A similar filter could be used to permit Telnet or WWW access. Set the Dest. Port ID to 23 for Telnet or 80 for WWW.

Firewall tutorial

General Firewall Terms

Firewall: a component or set of components that restrict access between a protected network and the Internet, or between two networks.

Host: A workstation on the Network.

Packet: Unit of communication on the Internet.

Packet Filter: Packet filters allow or deny packets based on source or destination IP addresses, TCP or UDP ports, or the TCP ACK bit.

Port: A number that defines a particular type of service.

Filter Rule: A filter set is comprised of individual filter rules.

Filter Set: A grouping of individual filter rules.

Basic IP Packet Components

All IP packets contain the same basic "header" information, as follows:

Source IP Address	163.176.132.18
Destination IP Address	163.176.4.27

Source Port	2541
Destination Port	80
Protocol	TCP
ACK Bit	Yes
DATA	User Data

This header information is what the packet filter uses to make filtering decisions. It is important to note that a packet filter does not look into the IP datastream (the User Data from above) to make filtering decisions.

Basic Protocol Types

TCP: Transmission Control Protocol. TCP provides reliable packet delivery and has a retransmission mechanism (so packets are not lost). RFC 793 is the specification for TCP.

UDP: User Datagram Protocol. Unlike TCP, UDP does not guarantee reliable, sequenced packet delivery. If data does not reach its destination, UDP does not re transmit the data. RFC 768 is the specification for UDP.

And there are many more ports defined in the Assigned Addresses RFC.

Example TCP/UDP Ports

TCP Port	Service	UDP Port	Service
20/21	FTP	161	SNMP
23	Telnet	69	TFTP
25	SMTP		
80	WWW		
144	News		

Firewall design rules

There are two basic rules to firewall design:

- “What is not explicitly allowed is denied...”

and

- “What is not explicitly denied is allowed...”

The first rule is far more secure, and is the best approach to firewall design. It is far easier (and more secure) to allow in or out only certain services and deny anything else. If the other rule is used, you would have to figure out everything that you want to disallow, now and future.

Firewall Logic

Firewall design is a test of logic, and filter rule ordering is critical. If a packet is passed through a series of filter rules and then the packet matches a rule, the appropriate action is taken. The packet will not pass through the remainder of the filter rules.

For example, if you had the following filter set...

Allow WWW access;

Allow FTP access;

Allow SMTP access;

Deny all other packets.

and a packet goes through these rules destined for FTP, the packet would pass through the first rule (WWW), go through the second rule (FTP), matches this rule and the packet is allowed through.

If you had this filter set for example....

Allow WWW access;

Allow FTP access;

Deny FTP access;

Deny all other packets.

and a packet goes through these rules destined for FTP, the packet would pass through the first filter rule (WWW), match the second rule (FTP) and the packet is allowed through. Even though the next rule is to deny all FTP traffic, the FTP packet will never make it to this rule.

Binary Representation

It is easiest when doing filtering to convert the IP address and mask in question to binary. This will allow you to perform the logical AND to determine if a packet matches a filter rule.

Logical ANDing

When a packet is compared (in most cases) a logical AND is performed. First the IP addresses and subnet masks are converted to binary and then ANDed together. The rules for logical ANDing are as follows:

0 AND 0 = 0

0 AND 1 = 0

1 AND 0 = 0

1 AND 1 = 1

For example:

Filter rule:

Deny

IP: 163.176.1.15 BINARY: 10100011.10110000.00000001.00001111

Mask: 255.255.255.255 BINARY: 11111111.11111111.11111111.11111111

Incoming Packet:

IP 163.176.1.15 BINARY: 10100011.10110000.00000001.00001111

AND the incoming packet and subnet mask together, the result is:

10100011.10110000.00000001.00001111

which matches the IP address in the filter rule and the packet is denied.

Implied Rules

With a given set of filter rules, there is an Implied rule which may or may not be shown to the user. The implied rule tells the filter set what to do with a packet that does not match any of the filter rules. An example of implied rules is as follows:

Implied	Meaning
Y+Y+Y=N	If all filter rules are YES, the implied is NO.
N+N+N=Y	If all filter rules are NO, the implied is YES.
Y+N+Y=N	If a mix of YES and NO filters, the implied is NO.

Established Connections

The TCP header contains one bit called the ACK Bit (or TCP Ack bit). This ACK Bit only appears with TCP, not UDP. The ACK bit is part of the TCP mechanism that guaranteed the delivery of data. The ACK bit is set whenever one side of a connection has received data from the other side. Only the first TCP packet will not have the ACK bit set, once the TCP connection is in place the remainder of the TCP packets with have the ACK bit set.

The ACK bit is helpful for firewall design and reduces the number of potential filter rules. A filter rule could be created just allowing incoming TCP packets with the ACK bit set, as these packets had to be originated from the local network.

Example IP Filter Set Screen

This is an example of the Netopia IP filter set screen:

```
                                Change Filter

          Enabled:                              Yes
          Forward:                              No

          Source IP Address:                    0.0.0.0
          Source IP Address Mask:               0.0.0.0

          Dest. IP Address:                     0.0.0.0
          Dest. IP Address Mask:                0.0.0.0

          Protocol Type:                        TCP

          Source Port Compare...                No Compare
          Source Port ID:                       0
          Dest. Port Compare...                 Equal
          Dest. Port ID:                        2000
          Established TCP Conns. Only:          No


Return/Enter accepts * Tab toggles * ESC cancels.
Enter the IP specific information for this filter.
```

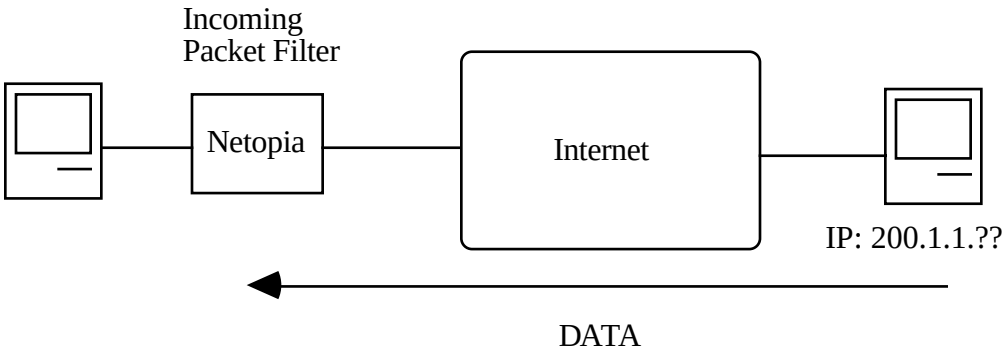
Filter Basics

In the source or destination IP address fields, the IP address that is entered MUST be the NETWORK address of the subnet. A HOST address can be entered, but the applied subnet mask must be 32 bits (255.255.255.255).

The Netopia R310 has the ability to compare source and destination TCP or UDP ports. These options are as follows:

Item	What it means
No compare	Does not compare TCP or UDP port
Not Equal To	Matches any port other than what is defined
Less Than	Anything less than the port defined
Less Than Or Equal	Any port less than or equal to the port defined
Equal	Matches only the port defined
Greater Than or Equal	Matches the port or any port greater
Greater Than	Matches anything greater than the port defined.

Example Network



Example Filters

Example 1

Filter Rule:	200.1.1.0	(Source IP Network Address)
	255.255.255.128	(Source IP Mask)
	Forward = No	(What happens on match)

Incoming packet has the source address of 200.1.1.28

IP Address	Binary Representation	
200.1.1.28	00011100	(Source address in incoming IP packet)
AND		
255.255.255.128	10000000	(Perform the logical AND)
	00000000	(Logical AND result)

This incoming IP packet has a source IP address that matches the network address in the Source IP Address field (00000000) in the Netopia R310. This will NOT forward this packet.

Example 2

Filter Rule:	200.1.1.0	(Source IP Network Address)
	255.255.255.128	(Source IP Mask)
	Forward = No	(What happens on match)

Incoming packet has the source address of 200.1.1.184

IP Address	Binary Representation	
200.1.1.184	10111000	(Source address in incoming IP packet)
AND		
255.255.255.128	10000000	(Perform the logical AND)
	10000000	(Logical AND result)

This incoming IP packet (10000000) has a source IP address that does not match the network address in the Source IP Address field (00000000) in the Netopia R310. This rule WILL forward this packet because the packet does not match.

Example 3

Filter Rule:	200.1.1.96	(Source IP Network Address)
	255.255.255.240	(Source IP Mask)
	Forward = No	(What happens on match)

Incoming packet has the source address of 200.1.1.184

IP Address	Binary Representation	
200.1.1.184	10111000	(Source address in incoming IP packet)
AND		
255.255.255.240	11110000	(Perform the logical AND)
	10110000	(Logical AND result)

Since the Source IP Network Address in the Netopia R310 is 01100000, and the source IP address after the logical AND is 1011000, this rule does NOT match and this packet will be passed.

Example 4

Filter Rule:	200.1.1.96	(Source IP Network Address)
	255.255.255.240	(Source IP Mask)
	Forward = No	(What happens on match)

Incoming packet has the source address of 200.1.1.104

IP Address	Binary Representation	
200.1.1.104	01101000	(Source address in incoming IP packet)
AND		
255.255.255.240	11110000	(Perform the logical AND)
	01100000	(Logical AND result)

Since the Source IP Network Address in the Netopia R310 is 01100000, and the source IP address after the logical AND is 01100000, this rule DOES match and this packet will NOT be passed.

Example 5

Filter Rule:	200.1.1.96	(Source IP Network Address)
	255.255.255.255	(Source IP Mask)
	Forward = No	(What happens on match)

Incoming packet has the source address of 200.1.1.96

IP Address	Binary Representation	
200.1.1.96	01100000	(Source address in incoming IP packet)
AND		
255.255.255.255	11111111	(Perform the logical AND)
	01100000	(Logical AND result)

Since the Source IP Network Address in the Netopia R310 is 01100000, and the source IP address after the logical AND is 01100000, this rule DOES match and this packet will NOT be passed. This rule masks off a SINGLE IP address.

Token Security Authentication

This section discusses how to configure and use security authentication on the Netopia R310.

Note: The security authentication feature only applies to Netopia R310 models connecting over a dial-up line using the PPP-PAP-TOKEN or PPP-CACHE-TOKEN authentication protocol.

Securing network environments

Unauthorized tampering or theft of information on internal networks causes serious ramifications, given the reliance on information systems. Network abuse is a serious problem, complicated by the difficulty in detecting the source of the abuses. An unauthorized user can gain access to networks and copy information without leaving a trace.

Password protection is one solution, but static passwords are often insecure. They can be compromised, allowing unauthorized users to disguise themselves as authorized users and enter supposedly secure systems. However, a company called Security Dynamics™ has patented a security authentication technology to increase network security.

SecurID is a two-factor authentication process to protect against unauthorized access. This dynamic user authentication produces a randomly-generated security code mechanism that changes every 60 seconds. At login, authorized users enter their password and the code displayed on their SecurID token card. While a password may be compromised, the constantly changing access code, which requires the token card during system use, bars unauthorized users from entering the network.

Using the SecurID token card

Each SecurID token card is programmed with an algorithm that ensures every code displayed is valid only for that user at that particular time. The token card has a display that authorizes the individual user access to the computer. Through this authentication system, the user's identity is verified when the correct password and current code are entered from the user's token.

Personal identification number (PIN)

The user's password is called a personal identification number, or PIN. The user enters the secret PIN from a console connection, followed by the current code displayed on the token card. Then the access control module must authenticate the token's unique code in combination with the user's secret PIN before access is granted.

Key Security Authentication Features of the Netopia R310

As a remote device, the Netopia R310 offers client/calling side security authentication. This feature allows the Netopia R310 to call a server router and perform security card authentication. The router of the called server must have access to a server with ACE software loaded on it.

To perform security card authentication, each user must have a security authentication token card and a PIN. In addition, the user's identifying information must reside on the remote ACE servers for authentication negotiation to properly take place.

The Netopia R310 supports the following user configurations for security authentication:

- Single user, calling a single destination (single session)
- Single user, calling multiple destinations (two simultaneous and separate sessions)
- Multiple users, calling a single destination (single session)
- Multiple users, calling multiple destinations (two simultaneous and separate sessions

Security authentication components

To properly identify and authenticate an authorized user, the following are required:

- A secret personal identification number (PIN) for each user.
- A security authentication token card.
- A Security Access Control Module (ACM).

Note: The Netopia R310 currently only supports Ascend routers as ACMs.

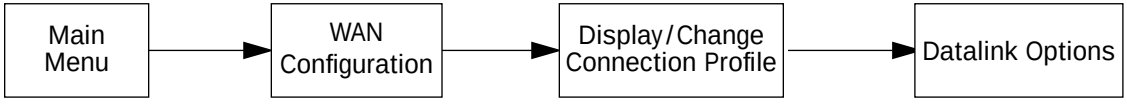
- An external Netopia R310 calling into a designated server. For example, a telecommuter dialing into a remote site from a Netopia R310 interested in accessing personal email or file sharing services.

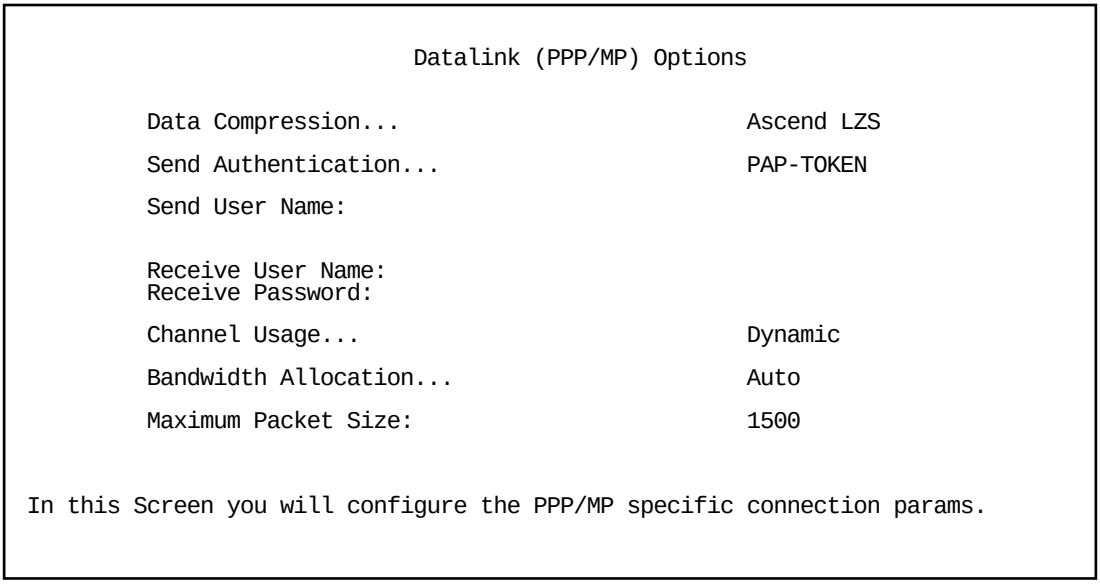
Note: The Netopia R310 does not include a security authentication token card.

Configuring for security authentication

To configure the Netopia R310 to support security authentication, select an authentication method and set up a designated connection profile from the System Configuration screen or your first connection profile from Easy Setup.

1. From the WAN Configuration menu, select Display/Change Connection Profile. From the pop-up menu that appears, select a Connection Profile. In the Connection Profile screen select **Datalink Options**.





2. Select Send Authentication and press Return. From the pop-up menu, highlight **PAP-TOKEN** or **CACHE-TOKEN**. Your network administrator or the remote network administrator will tell you which method to select.

   If you select PAP-TOKEN, select **Send User Name** and enter a name for your Netopia R310. You will not need to enter a Send Password for PAP-TOKEN. Press Return.

   If you select CACHE-TOKEN, select **Send User Name** and enter a name for your Netopia R310. Then, select **Send Password** and enter a secret name or number. Press Return.

3. Set up a connection profile to use with your authentication method. For information on setting up a connection profile, see Chapter 6, "Easy Setup."

Note: If you are setting up your first connection profile, you can also enter your authentication information in the Easy Setup Connection Profile screen.

Connecting using security authentication

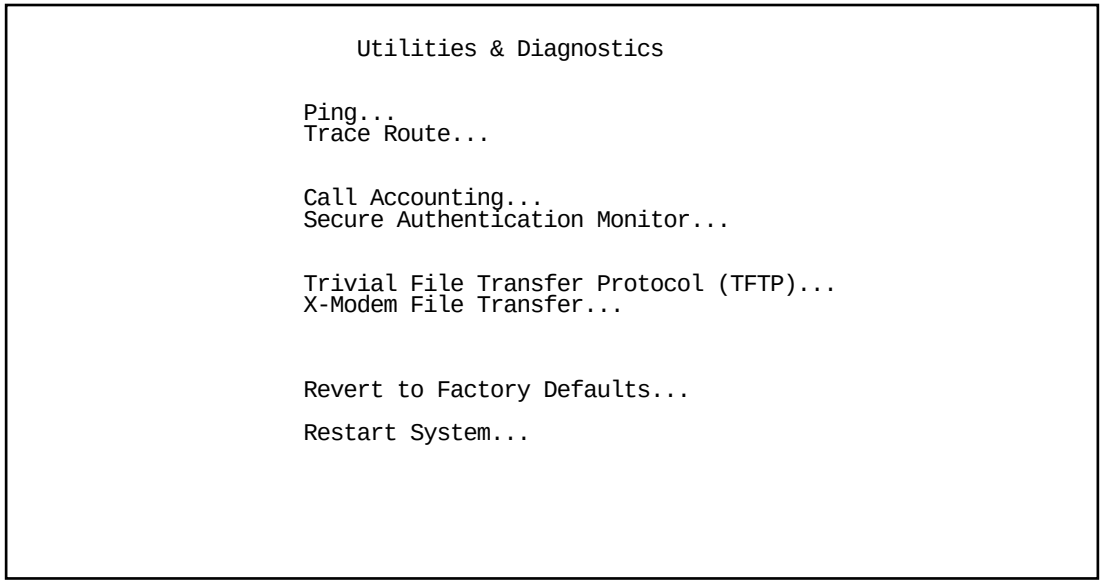
You can initiate a connection call using security authentication in either of two ways:

- establish a dial-on-demand (DOD) connection, or
- establish a manual connection.

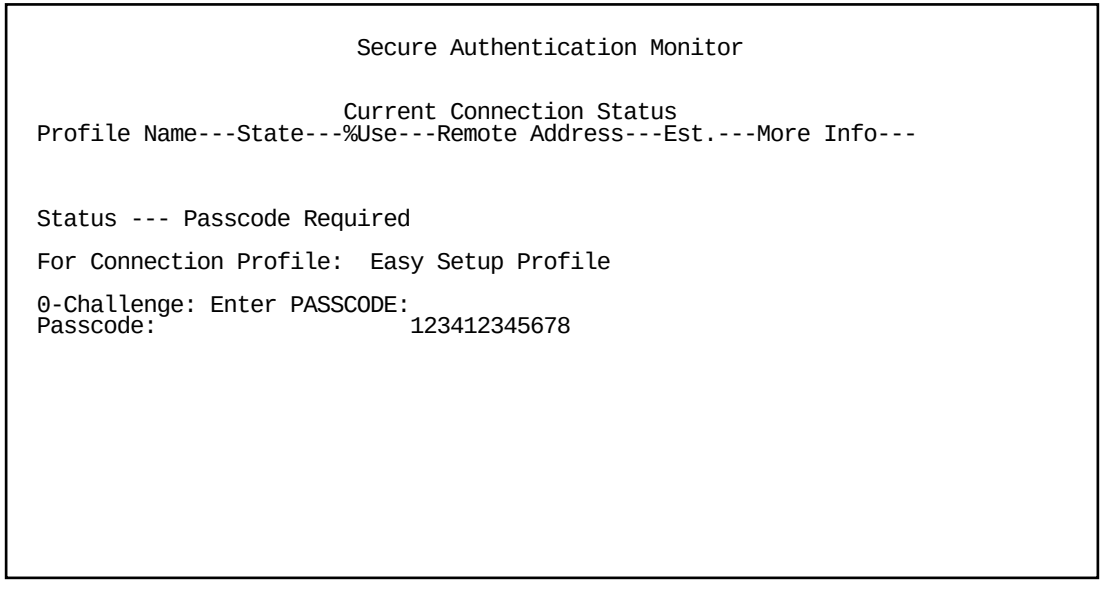
Establishing a dial-on-demand (DOD) connection call

To establish a connection call using DOD, select Utilities & Diagnostics from the Main Menu and press Return.

Note: The Secure Authentication Monitor field will remain hidden if PAP-TOKEN or CACHE-TOKEN is not the selected authentication method in the connection profile.



1. Select **Secure Authentication Monitor** and press Return. The Secure Authentication Monitor screen appears.
2. Wait for the call to initiate.



3. From the fields that appear, select **Enter PASSCODE** and press Return. Enter your PIN and the code displayed on your security authentication token card LED.
4. Once the call is established, and you enter your passcode as prompted, PPP negotiation will continue. If the call is specified for PAP-TOKEN, and the session involves more than one connection, you will be prompted for each connection being brought up.

Note: When using CACHE-TOKEN, your passcode is valid for a time interval determined by the network administrator. When this time interval expires, you must provide a new passcode for the call negotiation.

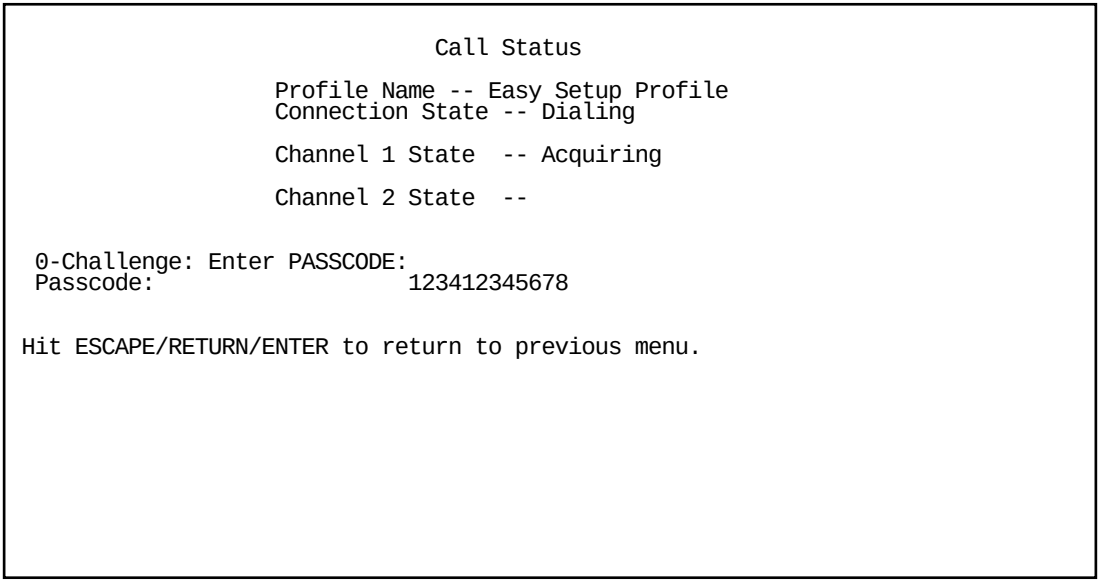
When using PAP-TOKEN, your passcode is valid for one call negotiation. For a second call negotiation, you must enter the next passcode provided by the security authentication token card every 60 seconds.

You will be able to access information at the remote site that you are connecting to once authentication is successfully completed.

Establishing a manual connection call

To establish a Manual connection call, select WAN Configuration from the Main Menu and press Return.

1. Select **Establish WAN Connection** from the WAN Configuration screen and press Return. The Establish WAN Connection screen displays a table of all of the connection profiles you have defined. Highlight the connection profile you wish to manually call. Press Return to initiate the call.



2. From the fields that appear, select **Enter PASSCODE** and press Return. Enter your PIN and the code displayed on your security authentication token card LED screen.
3. Once the call is established, and you enter your passcode as prompted, PPP negotiation will continue. If the call is specified for PAP-TOKEN, and the session involves more than one connection, you will be prompted for each channel being brought up.

Note: When using CACHE-TOKEN, your passcode is valid for a time interval determined by the network administrator. When this time interval expires, you must provide a new passcode for the call negotiation.

When using PAP-TOKEN for a dial-up call, your passcode is valid for one call negotiation. For a second call negotiation, you must enter the next passcode provided by the security authentication token card every 60 seconds.

You will be able to access information at the remote site that you are connecting to once authentication is successfully completed.

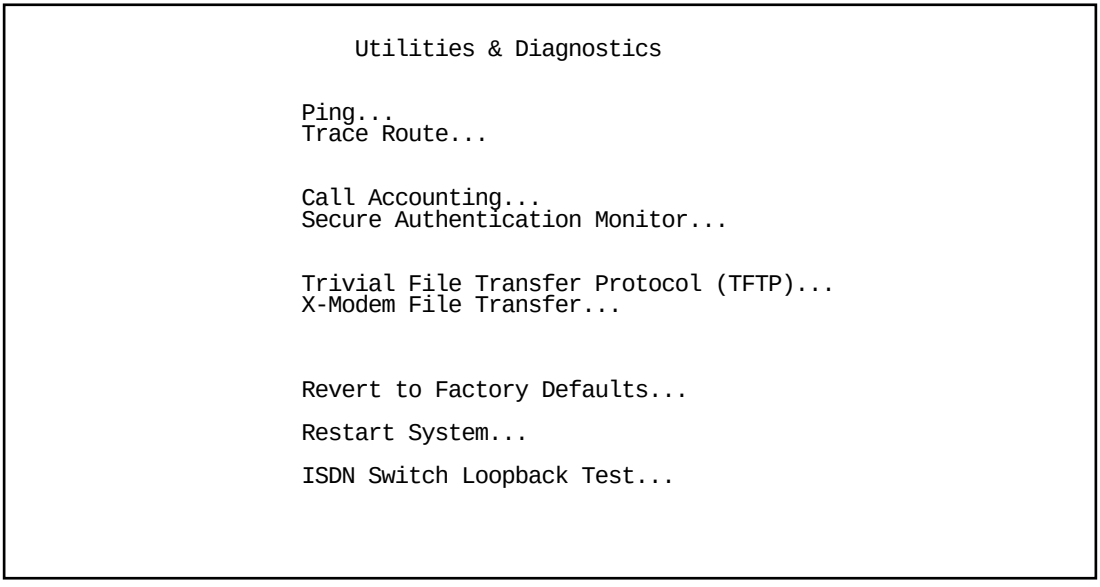
Chapter 13

Utilities and Diagnostics

A number of utilities and tests are available for system diagnostic and control purposes:

Note: These utilities and tests are accessible only through the console-based management screens. See Chapter 5, "Console-based Management," for information on accessing the console-based management screens.

You access the **Utilities & Diagnostics** screens from the **Main Menu**.

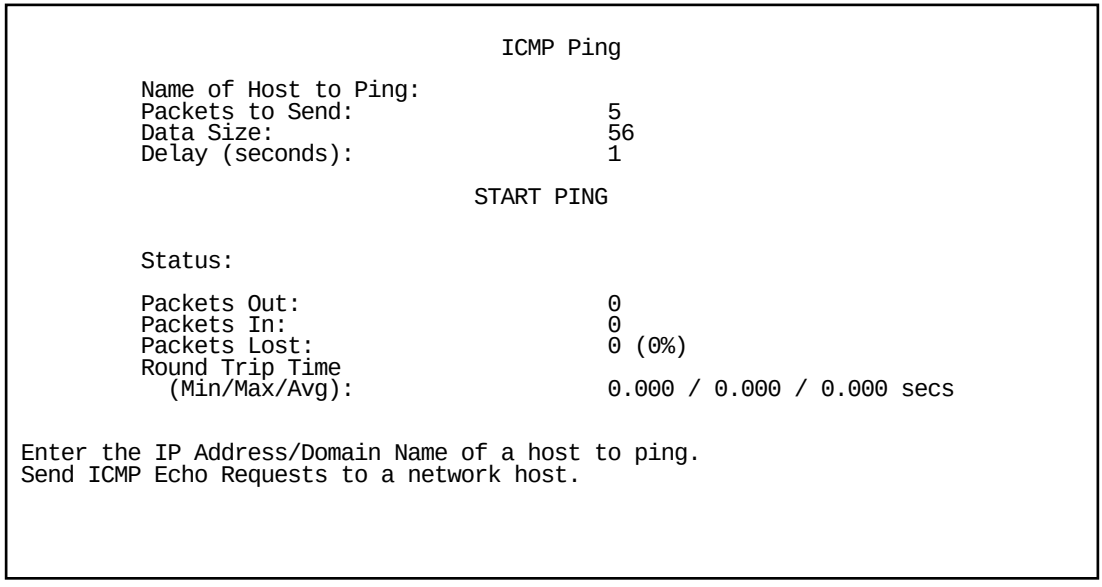


Ping

The Netopia R310 includes a standard Ping test utility. A Ping test generates IP packets destined for a particular (Ping-capable) IP host. Each time the target host receives a Ping packet, it returns a packet to the original sender.

Ping allows you to see whether a particular IP destination is reachable from the Netopia R310. You can also ascertain the quality and reliability of the connection to the desired destination by studying the Ping test's statistics.

To use the Ping utility, select **Ping** in the Statistics, Utilities, Tests screen and press Return to go to the Ping screen.



To configure and initiate a Ping test, follow these steps:

1. Select **Name of Host to Ping** and enter the destination domain name or IP address.
2. Select **Packets to Send** to change the default setting. This is the total number of packets to be sent during the Ping test. The default setting is adequate in most cases, but you may change it to any value from 1 to 4,294,967,295.
3. Select **Data Size** to change the default setting. This is the size, in bytes, of each Ping packet sent. The default setting is adequate in most cases, but you may change it to any value from 0 (only header data) to 1664.
4. Select **Delay (seconds)** to change the default setting. The delay, in seconds, determines the time between Ping packets sent. The default setting is adequate in most cases, but you may change it to any value from 0 to 4,294,967. A delay of 0 seconds forces packets to be sent immediately one after another.
5. Select **START PING** and press Return to begin the Ping test. While the test is running, the **START PING** item becomes **STOP PING**. To manually stop the Ping test, select **STOP PING** and press Return or the Escape key.

While the Ping test is running, and when it is over, a status field and a number of statistical items are active on the screen. These are described below.

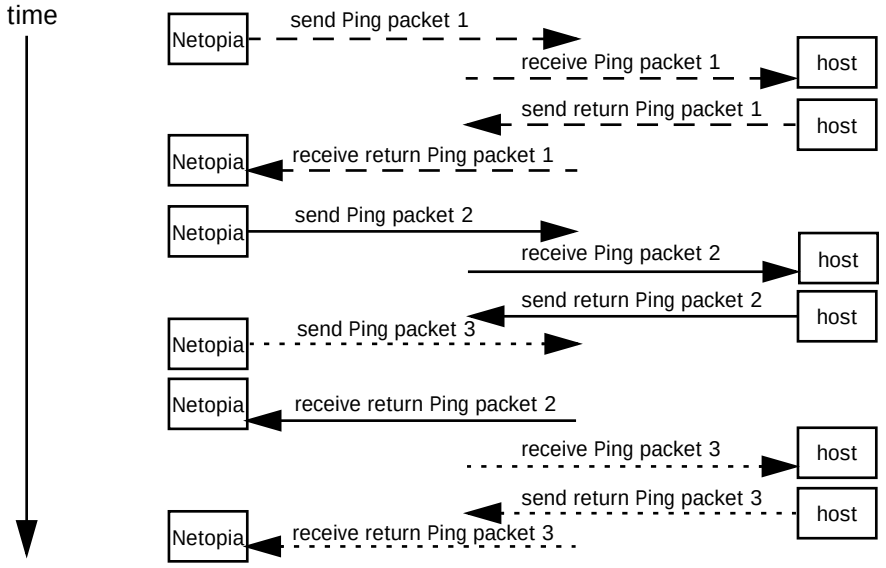
Status: The current status of the Ping test. This item can display the following messages:

Message	Description
Resolving host name	Finding the IP address for the domain name-style address
Can't resolve host name	IP address can't be found for the domain name-style name
Pinging	Ping test is in progress
Complete	Ping test was completed
Cancelled by user	Ping test was cancelled manually
Destination unreachable from w.x.y.z	Ping test was able to reach the router with IP address w.x.y.z, which reported that the test could not reach the final destination
Couldn't allocate packet buffer	Couldn't proceed with Ping test; try again or reset system
Couldn't open ICMP port	Couldn't proceed with Ping test; try again or reset system

Packets Out: The number of packets sent by the Ping test.

Packets In: The number of return packets received from the target host. To be considered "on time," return packets are expected back before the next packet in the sequence of Ping packets is sent. A count of the number of late packets appears in parentheses to the right of the **Packets In** count.

In the example below, a Netopia R310 is sending Ping packets to another host, which responds with return Ping packets. Note that the second return Ping packet is considered to be late because it is not received by the Netopia R310 before the third Ping packet is sent. The first and third return Ping packets are on time.



Packets Lost: The number of packets unaccounted for, shown in total and as a percentage of total packets sent. This statistic may be updated during the Ping test, and may not be accurate until after the test is over. However, if an escalating one-to-one correspondence is seen between **Packets Out** and **Packets Lost**, and **Packets In** is noticeably lagging behind **Packets Out**, the destination is probably unreachable. In this case, use **STOP PING**.

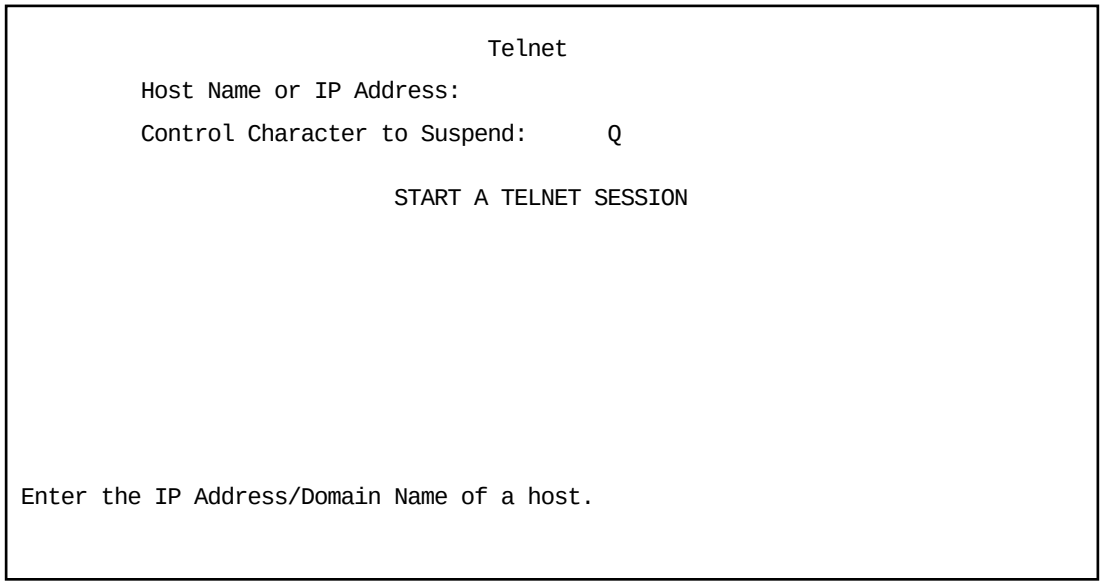
Round Trip Time (Min / Max / Avg): Statistics showing the minimum, maximum, and average number of seconds elapsing between the time each Ping packet was sent and the time its corresponding return Ping packet was received.

The time-to-live (TTL) value for each Ping packet sent by the Netopia R310 is 255, the maximum allowed. The TTL value defines the number of IP routers that the packet can traverse. Ping packets that reach their TTL value are dropped, and a "destination unreachable" notification is returned to the sender (see the table above). This ensures that no infinite routing loops occur. The TTL value can be set and retrieved using the SNMP MIB-II ip group's ipDefaultTTL object.

Telnet client

The Telnet client mode replaces the normal menu mode. Telnet sessions can be cascaded, that is, you can initiate a Telnet client session when using a Telnet console session. To activate the Telnet client, select **Telnet** from the Utilities & Diagnostics menu.

The Telnet client screen appears.



- Enter the host name or the IP address in dotted decimal format of the machine you want to telnet into and press Return.
- Either accept the default control character "Q" used to suspend the Telnet session, or type a different one.
- **START A TELNET SESSION** becomes highlighted.
- Press Return and the Telnet session will be initiated.
- To suspend the session, press Control-Q, or whatever other control character you specified.

  Two new options will appear in the Telnet screen (not shown):

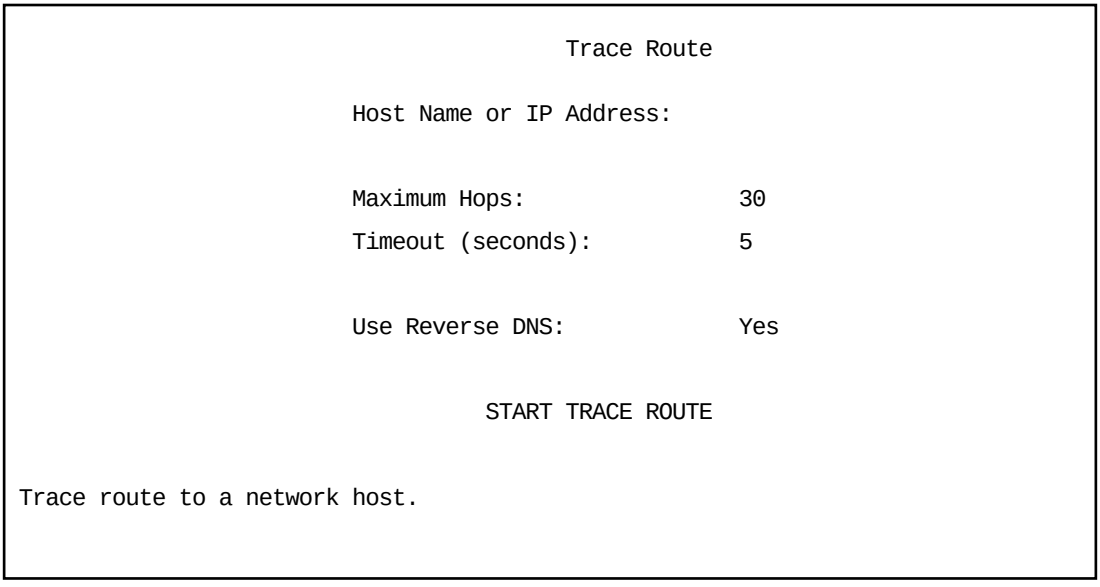
  Resume Suspended Session – select this one if you want to go back to your Telnet session

  Terminate Suspended Session – select this one if you want to end the session

Trace Route

You can count the number of routers between your Netopia Router and a given destination with the Trace Route utility.

Select **Trace Route** in the Statistics & Diagnostics screen and press Return to go to the Trace Route screen.



To trace a route, follow these steps:

1. Select **Host Name or IP Address** and enter the name or address of the destination you want to trace.
2. Select **Maximum hops (1..64)** to set the maximum number of routers to count between the Netopia Router and the destination router, up to the maximum of 64. The default is 30 hops.
3. Select **Timeout per probe (1..10 sec)** to set when the trace will timeout for each hop, up to 10 seconds. The default is 3 seconds.
4. Select **Use Reverse DNS** to learn the names of the routers between the Netopia Router and the destination router. The default is Yes.
5. Select **START TRACE ROUTE** and press Return. The screen will be replaced by a scrolling screen, listing the destination, the number of hops, the IP addresses of each hop, and the DNS names, if selected.
6. Cancel the trace by pressing Escape. Return to the Trace Route screen by pressing Escape twice.

Secure Authentication Monitor

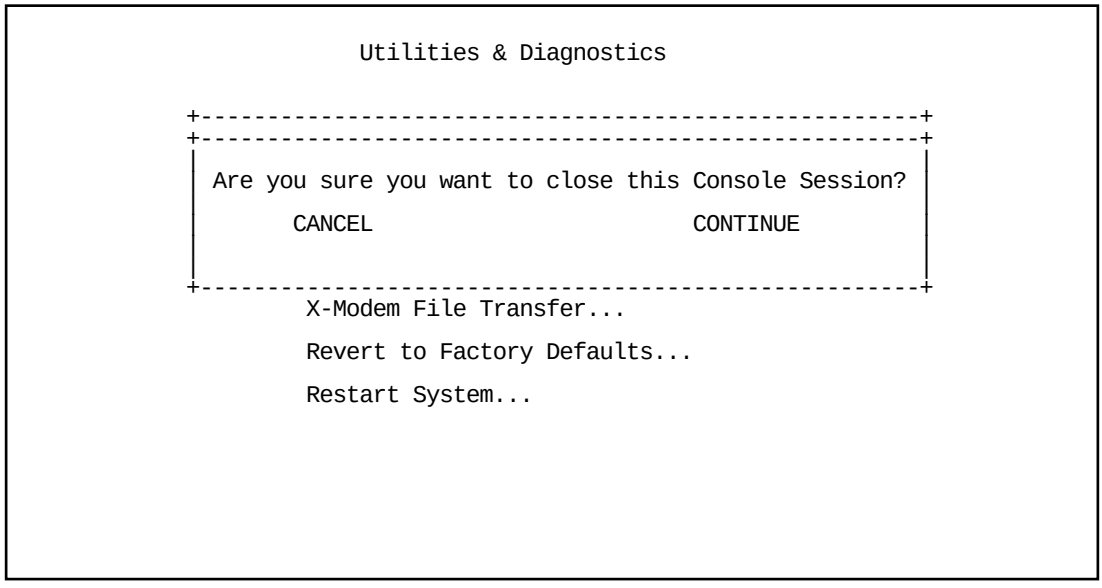
Note: The Secure Authentication Monitor field will remain hidden if PAP-TOKEN or CACHE-TOKEN is not the selected authentication method in the Connection Profile.

You use the Secure Authentication Monitor screen when placing one type of SecurID connection call. See "Connecting using security authentication" on page 12-32 for details.

Disconnect Telnet Console Session

If you want to close your Telnet Console session, select **Disconnect Telnet Console Session** and press Return.

A dialog box appears asking you to cancel or continue your selection.



If you select **Continue**, you will immediately terminate your session.

Factory defaults

You can reset the Netopia R310 to its factory default settings. Select the **Revert to Factory Defaults** item in the Statistics & Diagnostics screen and press Return. Select **CONTINUE** in the dialog box and press Return. The Netopia R310 will reboot and its settings will return to the factory defaults, deleting your configurations.

In an emergency, you can also use the Reset Switch to return the router to its factory default settings. Call Netopia Tech Support for instructions on using the Reset Switch.

Note: Reset to factory defaults with caution. You will need to reconfigure all your settings in the router.

Transferring configuration and firmware files with TFTP

Trivial File Transfer Protocol (TFTP) is a method of transferring data over an IP network. TFTP is a client-server application, with the Router as the client. To use the Router as a TFTP client, a TFTP server must be available. Netopia, Inc. has a public access TFTP server on the Internet where you can obtain the latest firmware versions.

To use TFTP, select **Trivial File Transfer Protocol (TFTP)** in the Statistics & Diagnostics screen and press Return to go to the Trivial File Transfer Protocol (TFTP) screen.

```
                Trivial File Transfer Protocol (TFTP)

        TFTP Server Name:

        Firmware File Name:

        GET ROUTER FIRMWARE FROM SERVER...

        Config File Name:

        GET CONFIG FROM SERVER...
        SEND CONFIG TO SERVER...

        TFTP Transfer State -- Idle

        TFTP Current Transfer Bytes -- 0
```

The sections below describe how to update the Router's firmware and how to download and upload configuration files.

Updating firmware

Firmware updates may be available periodically from Netopia or from a site maintained by your organization's network administrator.

The router firmware governs how the router communicates with your network and with the remote site. Router firmware updates are periodically posted on the Netopia website.

To update the router's firmware, follow these steps:

- Select **TFTP Server Name** and enter the server name or IP address of the TFTP server you will use. The server name or IP address is available from the site where the server is located.
- Select **Firmware File Name** and enter the name of the file you will download. The name of the file is available from the site where the server is located. You may need to enter a file path along with the file name (for example, bigroot/config/myfile).
- Select **Send Firmware to Netopia from TFTP Server** and press Return. You will see the following dialog box:

```
        +-----------------------------------------------------------+
        +-----------------------------------------------------------+
        |                                                           |
        |      Are you sure you want to read the firmware now?      |
        |      The device will reset when the transfer is complete. |
        |                                                           |
        |              CANCEL                CONTINUE               |
        |                                                           |
        +-----------------------------------------------------------+
```

- Select **CANCEL** to exit without downloading the file, or select **CONTINUE** to download the file. The system will reset at the end of the file transfer to put the new firmware into effect. While the system resets, the LEDs will blink on and off.

Caution!

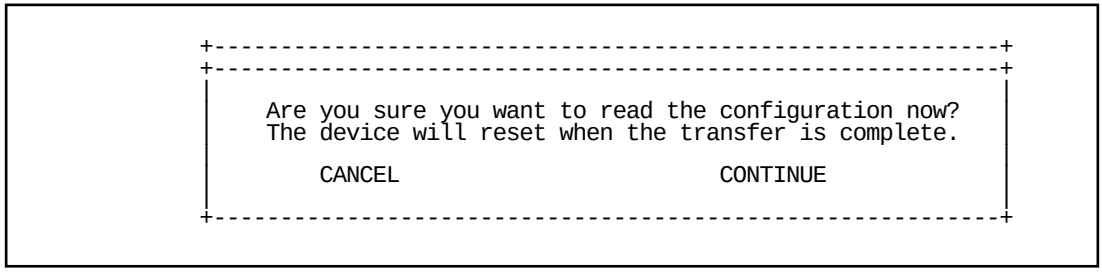
- Be sure the firmware update you load onto your router is the correct version for your particular model. Some models do not support all firmware versions. Loading an incorrect firmware version can permanently damage the unit.
- Do not manually power down or reset the Netopia R310 while it is automatically resetting or it could be damaged.
- If you choose to download the firmware, the **TFTP Transfer State** item will change from **Idle** to **Reading Firmware**. The **TFTP Current Transfer Bytes** item will reflect the number of bytes transferred.

Downloading configuration files

The Router can be configured by downloading a configuration file using TFTP. Once downloaded, the file reconfigures all of the Router's parameters as if someone had manually done so through the console port.

To download a configuration file, follow these steps:

- Select **TFTP Server Name** and enter the server name or IP address of the TFTP server you will use. The server name or IP address is available from the site where the server is located.
- Select **Config File Name** and enter the name of the file you will download. The name of the file is available from the site where the server is located. You may need to enter a file path along with the file name (for example, bigroot/config/myfile).
- Select **Read Config Now** and press Return. You will see the following dialog box:



- Select **CANCEL** to exit without downloading the file, or select **CONTINUE** to download the file. The system will reset at the end of the file transfer to put the new configuration into effect.
- If you choose to download the configuration file, the **TFTP Transfer State** item will change from **Idle** to **Reading Config**. The **TFTP Current Transfer Bytes** item will reflect the number of bytes transferred.

Uploading configuration files

Using TFTP, you can send a file containing a snapshot of the Router's current configuration to a TFTP server. The file can then be downloaded by a different Netopia R310 unit to configure its parameters (see "Downloading configuration files" on page 13-9). This is useful for configuring a number of Routers with identical parameters, or just for creating configuration backup files.

Uploading a file can also be useful for troubleshooting purposes. The uploaded configuration file can be tested on a different Netopia R310 unit by Netopia or your network administrator.

To upload a configuration file, follow these steps:

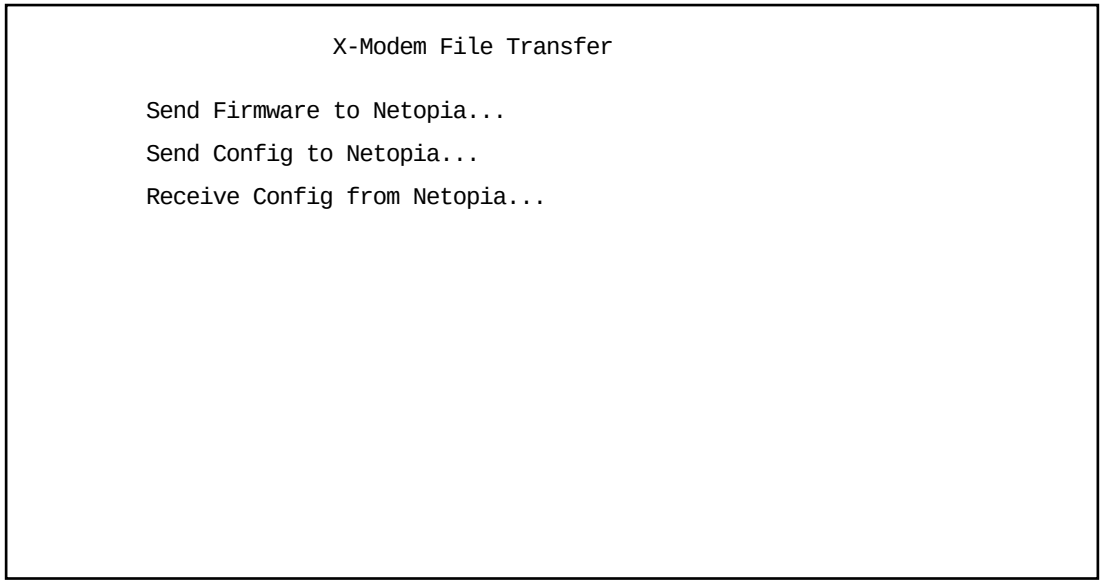
1. Select **TFTP Server Name** and enter the server name or IP address of the TFTP server you will use. The server name or IP address is available from the site where the server is located.
2. Select **Config File Name** and enter a name for the file you will upload. The file will appear with the name you choose on the TFTP server. You may need to enter a file path along with the file name (for example, Mypc/Netopia/myfile).
3. Select **Write Config Now** and press Return. Netopia will begin to transfer the file.
4. The **TFTP Transfer State** item will change from **Idle** to **Writing Config**. The **TFTP Current Transfer Bytes** item will reflect the number of bytes transferred.

Transferring configuration and firmware files with XMODEM

You can transfer configuration and firmware files with XMODEM through the Netopia R310's console port. Be sure your terminal emulation program supports XMODEM file transfers.

To go to the **X-Modem File Transfer** screen, select it in the Utilities & Diagnostics screen.

Note: The X-Modem File Transfer screen is only available if you are connected via the Console port.

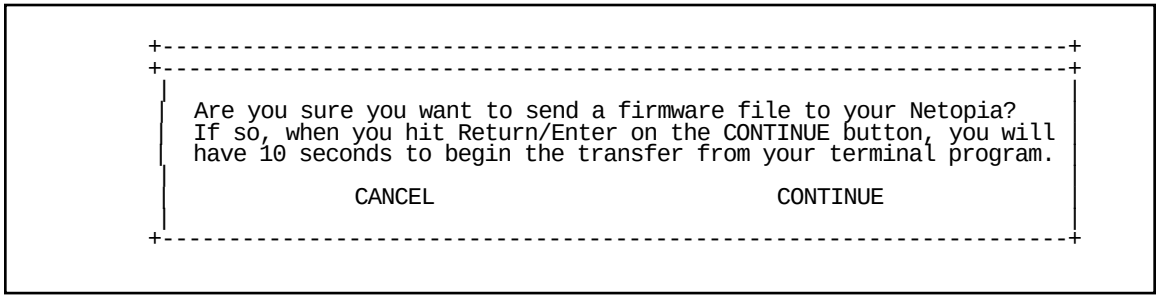


Updating firmware

Firmware updates may be available periodically from Netopia or from a site maintained by your organization's network administration.

Follow these steps to update the Netopia R310's firmware:

1. Make sure you have the firmware file on disk and know the path to its location.
2. Select **Send Firmware to Netopia** and press Return. The following dialog box appears:



3. Select **CANCEL** to exit without downloading the file, or select **CONTINUE** to download the file.

   If you choose **CONTINUE**, you will have ten seconds to use your terminal emulation software to initiate an XMODEM transfer of the firmware file. If you fail to initiate the transfer in that time, the dialog box will disappear and the terminal emulation software will inform you of the transfer's failure. You can then try again.

   The system will reset at the end of a successful file transfer to put the new firmware into effect. While the system resets, the LEDs will blink on and off.

Caution!

Do not manually power down or reset the Netopia R310 while it is automatically resetting or it could be damaged.

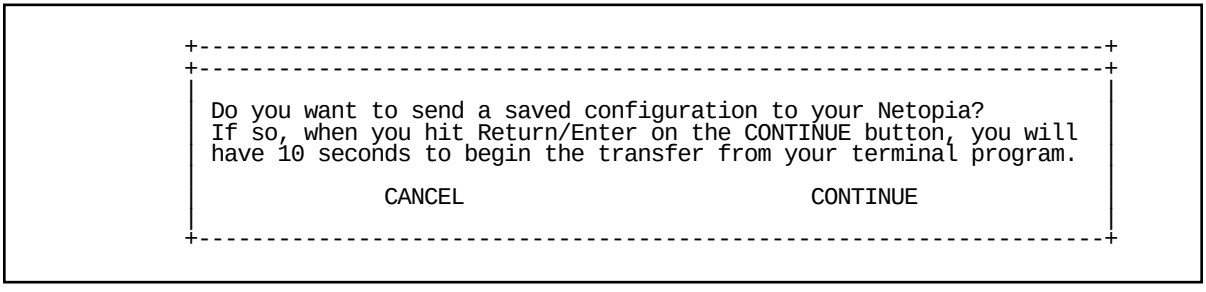
Downloading configuration files

The Netopia R310 can be configured by downloading a configuration file. The downloaded file reconfigures all of the Router's parameters.

Configuration files are available from a site maintained by your organization's network administrator or from your local site (see "Uploading configuration files," below).

Follow these steps to download a configuration file:

1. Make sure you have the configuration file on disk and know the path to its location.
2. Select **Send Config to Netopia** and press Return. The following dialog box appears:



3. Select **CANCEL** to exit without downloading the file, or select **CONTINUE** to download the file.

If you choose **CONTINUE**, you will have ten seconds to use your terminal emulation software to initiate an XMODEM transfer of the configuration file. If you fail to initiate the transfer in that time, the dialog box will disappear and the terminal emulation software will inform you of the transfer's failure. You can then try again.

The system will reset at the end of a successful file transfer to put the new configuration into effect.

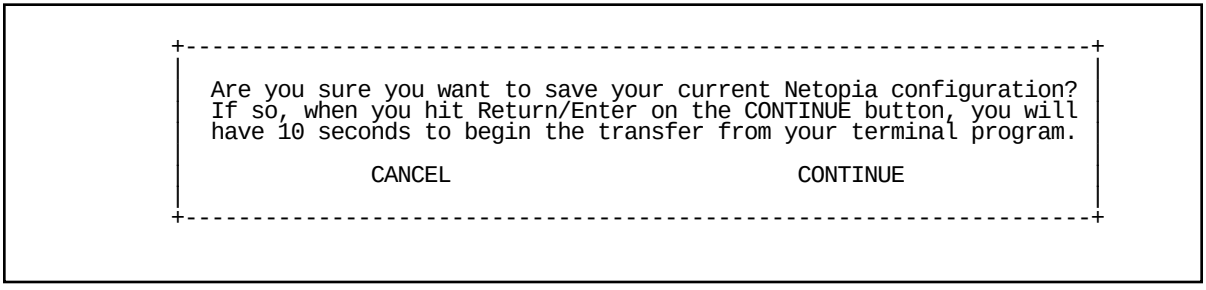
Uploading configuration files

A file containing a snapshot of the Netopia R310's current configuration can be uploaded from the Router to disk. The file can then be downloaded by a different Netopia R310 to configure its parameters (see "Downloading configuration files" on page 13-11). This is useful for configuring a number of Routers with identical parameters, or for creating configuration backup files.

Uploading a file can also be useful for troubleshooting purposes. The uploaded configuration file can be tested on a different Netopia R310 by Netopia or your network administrator.

To upload a configuration file:

1. Decide on a name for the file and a path for saving it.
2. Select **Receive Config from Netopia** and press Return. The following dialog box appears:



3. Select **CANCEL** to exit without uploading the file, or select **CONTINUE** to upload the file.

   If you choose **CONTINUE**, you will have ten seconds to use your terminal emulation software to initiate an XMODEM transfer of the configuration file. If you fail to initiate the transfer in that time, the dialog box will disappear and the terminal emulation software will inform you of the transfer's failure. You can then try again.

Restarting the system

You can restart the system by selecting the **Restart System** item in the Utilities & Diagnostics screen.

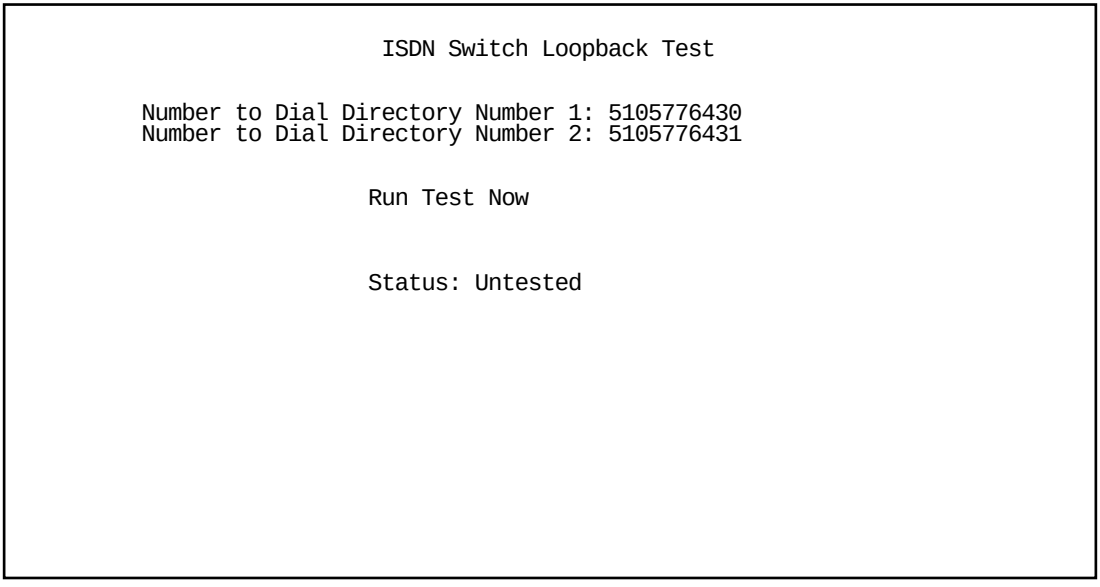
You must restart the system whenever you reconfigure the Netopia R310 and want the new parameter values to take effect. Under certain circumstances, restarting the system may also clear up system or network malfunctions. Some configuration processes automatically restart the system to apply the changes you have made.

ISDN Switch Loopback Test

The ISDN loopback test is designed to confirm the existence of a working ISDN line and the proper configuration of certain Netopia R310 ISDN Router parameters. This test is available only on switched ISDN lines.

Using the first B-channel, the test calls the Netopia R310 on the second B-channel, creating a call loop back to the unit.

To run the ISDN loopback test, select **ISDN Switch Loopback Test** in the Utilities & Diagnostics screen and press Return. The ISDN Switch Loopback Test screen appears.



Note: "Number to Dial Directory Number 1 and 2" fields are only visible if there are no DNs in the ISDN line configuration.

Select **Run Test Now** and press Return. The loopback test is executed immediately.

Note: Make sure neither B-channel is in use before you execute the loopback test.

The **Status** item reports one of three results:

Untested: The loopback test has not yet been run.

Loopback Test FAILED: The loopback test has failed. See “If the loopback test fails,” below, for troubleshooting suggestions.

Loopback Test PASSED. The loopback test was successful. The line is working properly, and the directory numbers (the ISDN phone numbers associated with each B-channel) are correct.

If the loopback test fails

Follow these suggestions to track down the reason behind the loopback test's failure:

- Check that the WAN Ready LED is solid green.
- Check the ISDN event log and get more information about events that seem relevant to the failure.
- Check the B-channel usage in the Quick View screen to make sure there were no active calls when the loopback test was performed.
- Check the accuracy of the directory numbers and switch protocol you entered in the ISDN Line Configuration screen (compare them with the information you received from your ISDN service provider).
- Verify termination of the S/T bus.
- Contact your ISDN service provider to have the line checked.
- Check that your line is not provisioned for voice only (Circuit Switched Voice).

Part III: Appendixes

Appendix A

Troubleshooting

This appendix is intended to help you troubleshoot problems you may encounter while setting up and using the Netopia R310. It also includes information on how to contact Netopia Technical Support.

Important information on these problems may be found in the event histories kept by the Netopia R310. These event histories can be accessed in the Statistics, Utilities, Tests screen.

This section covers the following topics:

Configuration problems

If you encounter problems during your initial configuration process, review the following suggestions before calling for technical support. There are four zones to consider when troubleshooting initial configuration:

1. the computer's connection to the router;
2. the router's connection to the telecommunication line(s);
3. the telecommunication line's connection to your ISP, and
4. the ISP's connection to the Internet.

If the connection from the computer to the router was not successful, check the following:

- The Netopia R310 is turned on.
- An Ethernet cable connects your PC's Ethernet card or built-in Ethernet port to the Netopia R310.
- The SmartStart application is running and able to access the Netopia R310.
- Telnet is available on your PC or Macintosh. (On a PC, it must be specified in your system path. You can usually find the application as "c:\windowselnet.exe".)
- Your PC or Macintosh has an IP address, either automatically or statically assigned, and compatible with the default IP address of the router, 198.162.1.1.
- Your PC or Macintosh has a subnet mask that matches or is compatible with the Netopia R310's default subnet mask, 255.255.255.0.
- If you are entering a new IP address via SmartStart be sure the correct serial number was entered.

SmartStart Troubleshooting

The Status field of the SmartStart application will display information and indicate problems as they are detected.

Console connection problems

Can't see the configuration screens (nothing appears)

- Check the cable connection from the Netopia R310's console port to the computer being used as a console.
- Check that the terminal emulation software is accessing the correct port on the computer that's being used as a console.
- Try pressing Ctrl-L or Return or the ▲ up or down▼ key several times to refresh the terminal screen.
- Check that flow control on serial connections is turned off.

Junk characters appear on the screen

- Check that the terminal emulation software is configured correctly.
- Check the baud rate. The default values are 9600, N, 8, and 1.

Characters are missing from some of the configuration screens

- Try changing the Netopia R310's default speed of 9600 bps and setting your terminal emulation software to match the new speed.

Network problems

This section contains tips on ways you can troubleshoot a networking problem.

Problems communicating with remote IP hosts

- Verify the accuracy of the default gateway's IP address (entered in the IP Setup or Easy Setup screen).
- Use the Netopia R310's ping utility, in the Statistics, Tests, Utilities screen, and try to ping local and remote hosts. See "Ping" on page 13-2 for instructions on how to use the ping utility. If you can successfully ping hosts using their IP addresses but not their domain names (198.34.7.1 but not garcia.netopia.com, for example), verify that the DNS server's IP address is correct and that it is reachable from the Netopia R310 (use ping).
- If you are using filters, check that your filter sets are not blocking the type of connections you are trying to make.

Local routing problems

- Observe the Ethernet LEDs to see if data traffic flow appears to be normal.
- Check the WAN Statistics and LAN Statistics screens to see more specific information on data traffic flow and address serving.

Power outages

If you suspect that power was restored after a power outage, and the Netopia R310 is connected to a remote site, you may need to switch the Netopia R310 off and then back on again. After temporary power outages, a connection that still seems to be up may actually be disconnected. Rebooting the router should reestablish the connection.

Technical support

Netopia, Inc. is committed to providing its customers with reliable products and documentation, backed by excellent technical support on-line and through our resellers and distributors.

Before contacting Netopia

Look in this guide for a solution to your problem. You may find a solution in this troubleshooting appendix or in other sections. Check the index for a reference to the topic of concern. If you cannot find a solution, complete the environment profile below before contacting technical support.

Environment profile

- Locate the Netopia R310's model number, product serial number, and firmware version. The serial number is on the bottom side of the Router, along with the model number. The firmware version appears in the Netopia R310's Main Menu screen.

  Model number:

  Serial number:

  Firmware version:

- What kind of local network(s) do you have, with how many devices?

  Ethernet

  LocalTalk

  EtherTalk

  TCP/IP

  IPX

  Other:

How to get support

We can help you with your problem more effectively if you have completed the environment profile in the previous section. If you contact your local reseller or distributor by telephone, please be ready to supply them with the information you used to configure the Netopia R310. Also, please be at the site of the problem and prepared to reproduce it and to try some troubleshooting steps.

You may also contact Netopia Technical Support directly by e-mail, telephone, fax, or post:

Internet: techsports@netopia.com (for technical support)
info@netopia.com (for general information)

Phone: 1 800-782-6449
Fax: 1 510-814-5023

Netopia, Inc.
Customer Service
2470 Mariner Square Loop
Alameda, California 94501
USA

Netopia Bulletin Board Service: 1 510-865-1321

Online product information

Product information can be found in the following:

Netopia World Wide Web server via http://www.netopia.com
Internet via anonymous FTP to ftp.netopia.com/pub

FAX-Back

This service provides technical notes which answer the most commonly asked questions, and offer solutions for many common problems encountered with Netopia products.

FAX-Back: +1 510-814-5040

Appendix B

Setting Up Telco Services

This chapter describes how to obtain telco services from your telephone service provider.

This section covers the following topics:

Obtaining an ISDN line

To obtain an ISDN line:

1. Find an ISDN service provider — see below.
2. Choose the type of ISDN line you need — see "Choosing an ISDN line" on page B-1
3. Order the ISDN line — see "Ordering an ISDN line" on page B-1.

Note: A worksheet is provided on page B-3 to simplify the procedure for obtaining an ISDN line.

Finding an ISDN service provider

Local telephone companies, long-distance telephone companies or other vendors may provide ISDN service. If you are unsure of who provides ISDN service in your area, contact your local telephone company.

Choosing an ISDN line

- Order an ISDN line that supports both data and voice. Some providers charge less for voice provisioning.

Ordering an ISDN line

The following sections provide items to consider when ordering an ISDN line.

The physical ISDN line

You can either convert an existing analog telephone line to ISDN or install a new ISDN line.

In either case, make sure there is a wall jack for the line near the location where you intend to install the Netopia Router.

In many cases, ISDN can use the same physical wire used for analog service. For more information consult with your ISDN service provider.

Note: You cannot connect analog equipment, such as telephones, facsimile machines, and modems directly into an ISDN line, without special equipment.

If your site has only one telephone line, we recommend you keep the existing analog line to conduct non-ISDN communications.

Setup tips

Your ISDN service provider may have the Netopia Router on a list of supported products that have been tested with a particular ISDN line configuration. Your ISDN service provider will know how to set up your line if the Netopia Router is on that list.

Switch protocol type

To configure the Netopia Router, your ISDN service provider must provide you with the switch protocol type used on your ISDN line.

The Netopia Router supports the following protocols:

- EuroISDN (also known as ETSI or NET3)
- Japanese NTT
- Australian TS013

Testing the ISDN line

Once the Netopia Router is installed and configured, use the loopback test to evaluate the line. See "ISDN Switch Loopback Test" on page 13-13. If the line does not work properly, ask your ISDN service provider to reconfigure the line until it works properly. A successful loopback is necessary for a bonded 128K 2B connection.

Completing the ISDN worksheet

The following ISDN worksheets are provided for you to enter ISDN account information. For your convenience, you may want to photocopy the appropriate ISDN worksheet, and then complete the copy.

When completing the worksheet, fill in:

- Section 1 when you find out from whom you'll be ordering your ISDN line.
- Section 2 when ordering your ISDN line.
- Section 3 after ordering your ISDN line.

Complete the worksheet carefully. You will need this information when configuring the Netopia Router.

Have the worksheet available if you call Netopia Technical Support. The information on the sheet will help a Netopia technician answer your questions quickly.

Note: The ISDN worksheet is for your convenience only. You may receive forms containing similar information from your ISDN service provider. The ISDN worksheet is neither an application for an ISDN line nor a substitute for the forms your ISDN service provider uses.

ISDN Telco Worksheet

1. ISDN Service Provider (Telephone Company) contact information

Name and Address:

_____

_____

Telephone/Fax numbers: _____

E-mail address: _____

2. Your information

Street address where your ISDN line is located:

_____

_____

Contact person at this location, including phone number:

_____

Is this an existing line or a new line (to be installed)? __ existing __ new

List the number in the telephone company's directory? __ no __ yes

Billing address for your ISDN line:

_____

_____

3. ISDN information

ISDN line configuration method used (check one):

__ By product (Netopia Router) __ Other method

Type of switch (check one):

__ EuroISDN (ETSI, NET3)

— Japanese NTT

— Australia TS013

Primary directory number (ID 1): _____

Secondary directory number (ID 2): _____

Type of services (check one)

__ voice and data (B 1) __ voice and data (B 2) __ data only

Appendix C

Setting Up Internet Services

This chapter describes how to obtain and set up Internet Services.

This section covers the following topics:

Note: Some companies act as their own ISP. For example, some organizations have branch offices that can use the Netopia R310 to access the Internet via the main office in a point-to-point scenario. If you install the Netopia R310 in this type of environment, refer to the following sections for specific information you must receive from the network administrator to configure the Netopia R310 properly.

Finding an Internet service provider

Internet access is available from Internet service providers (ISPs). Typically, there are several ISPs in each area. To locate ISPs in your area, consult your telephone book, local computer magazines, the business section of a local newspaper, or the following URL on the Internet: 'http://www.thelist.com'. Also see Netopia's home page at 'http://www.netopia.com' for a list of special programs and promotions for Netopia customers.

If your area has more than one ISP, the following considerations may help you decide which ISP is best suited for your requirements.

Use an ISP that provides Internet access through a digital line that supports the following:

Type of Service	Data Rate Speed	Datalink Protocol
ISDN	56/64-128 kbps	PPP or HDLC

Unique requirements

Make sure the ISP can meet any unique requirements you may have. Potential requirements include:

- Dynamic or static IP addressing
- Class C IP address
- Custom domain name
- Multiple email addresses
- Web site hosting
- Call back for web site hosting at your site

Pricing and support

Compare pricing, service, and technical support service among various ISPs.

ISP's Point of presence

Check with your ISP for the location of their nearest point of presence (POP) in reference to your site. In some instances, the ISP that you choose may not offer a POP in your local area. If that is the case, you may incur additional fees for long-distance calls.

Endorsements

Consider recommendations from colleagues and reviews in publications. Netopia lists Netopia Certified ISPs on our web site at 'http://www.netopia.com'.

Deciding on an ISP account

Your ISP may offer various Internet access account plans. Typically, these plans vary by usage charges and the number of host IP addresses supplied. Evaluate your networking needs and discuss them with your ISP before deciding on a plan for your network.

The following checklist is a guide to ensure you obtain the Internet service you require.

Setting up a Netopia R310 account

Check whether your ISP has the Netopia R310 on a list of supported products that have been tested with a particular configuration. If the ISP does not have the Netopia R310 on such a list, describe the Netopia R310 in as much detail as needed, so your ISP account can be optimized. As appropriate, you may refer your ISP to Netopia's web site for more information.

Obtaining an IP host address

Typically, each computer on the network that requires Internet access requires its own unique IP address. If some or all network computers require simultaneous Internet access, obtain a block of IP host addresses large enough for each computer to have its own address, plus one for the Netopia R310.

Consider expected growth in your network when deciding on the number of addresses to obtain. Alternatively, you may use the Network Address Translation feature of SmartIP.

SmartIP™

The Netopia R310 ISDN Router supports the SmartIP™ feature which includes Network Address Translation.

Network Address Translation provides Internet access to the network connected to the Netopia R310 using only a single IP address. These routers translate between the internal or local area network (LAN) addresses and a single external IP address and route accordingly.

For more information on Network Address Translation, see Chapter 9, "IP Setup and Network Address Translation."

Obtaining information from the ISP

After your account is set up, the ISP should send you the IP parameter information that will help you to configure the Netopia R310.

Local LAN IP address information to obtain

With Network Address Translation

If you are using SmartIP (NAT), you should obtain the following:

- If you are dialing out to a remote site using Network Address Translation on your router, your provider will not define the IP address information on your local LAN. You can define this information based on parameters defined by another connection profile such as that to a corporate network, or an IP configuration that may already be in place for the existing network. Alternatively, you can use the default IP address range used by the router.
- Primary and Secondary Domain Name Server (DNS) IP Addresses
- Domain Name (usually the same as the ISP's domain name unless you have registered for your own individual domain name)

Remote WAN IP address information to obtain

- Telephone number of the ISP's local or nearby dial-up POP (point-of-presence).
- PPP authentication type for router at the ISP, such as PAP.
- Send and receive User Login name and Send and receive User Password if PAP or CHAP security authentication is used

Without Network Address Translation

If you are not using SmartIP (NAT), you should obtain:

- The number of Ethernet IP host addresses available with your account and the first usable IP host address in the address block
- The Ethernet IP address for your Netopia R310
- The Ethernet IP subnet mask address for your Netopia R310
- The Default Gateway IP Address (same as Remote IP Address in most cases)
- Primary and Secondary Domain Name Server IP Addresses
- Domain Name (usually the same as the ISP's domain name unless you have registered for your own individual domain name)

Note: If you are not using Network Address Translation, you will need to obtain all of the Local LAN IP address information from your ISP.

Remote WAN IP address information to obtain

- The telephone number of the ISP's local or nearby dial-up POP (point-of-presence).
- Remote IP address of router at ISP or other remote site
- Remote IP subnet mask address of router at ISP or other remote site
- PPP authentication type for router at the ISP, such as PAP.
- Send User Login name and Send User Password if PAP or CHAP security authentication is used

Note: If you are not using Network Address Translation, you will need to obtain all of the Remote WAN IP address information from your ISP.

Appendix D

Understanding IP Addressing

This appendix is a brief general introduction to IP addressing. A basic understanding of IP will help you in configuring the Netopia R310 and using some of its powerful features, such as static routes and packet filtering.

In packets, a header is part of the envelope information that surrounds the actual data being transmitted. In e-mail, a header is usually the address and routing information found at the top of messages.

This section covers the following topics:

What is IP?

All networks use protocols to establish common standards for communication. One widely used network protocol is the Internet Protocol, also known as IP. Like many other protocols, IP uses packets, or formatted chunks of data, to communicate.

Note: This guide uses the term "IP" in a very general and inclusive way, to identify all of the following:

- Networks that use the Internet Protocol, along with accompanying protocols such as TCP, UDP, and ICMP
- Packets that include an IP header within their structure
- Devices that send IP packets

About IP addressing

Every networking protocol uses some form of addressing in order to ensure that packets are delivered correctly. In IP, individual network devices that are initial sources and final destinations of packets are usually called hosts, instead of nodes, but the two terms are interchangeable. Each host on an IP network must have a unique IP address. An IP address, also called an Internet address, is a 32-bit number usually expressed as four decimal numbers separated by periods. Each decimal number in an IP address represents a 1-byte (8-bit) binary number. Thus, values for each of the four numbers range from 00000000 to 11111111 in binary notation, or from 0 to 255 in decimal notation. The expression 192.168.1.1 is a typical example of an IP address.

IP addresses indicate both the identity of the network and the identity of the individual host on the network. The number of bits used for the network number and the number of bits used for the host number can vary, as long as certain rules are followed. The local network manager assigns IP host numbers to individual machines.

IP addresses are maintained and assigned by the InterNIC, a quasi-governmental organization now increasingly under the auspices of private industry.

Note: It's very common for an organization to obtain an IP address from a third party, usually an Internet service provider (ISP). ISPs usually issue an IP address when they are contracted to provide Internet access services.

The InterNIC (the NIC stands for Network Information Center) divides IP addresses into several classes. Classes A, B, and C are assigned to organizations who request addresses. In Class A networks, the first byte of an IP address is reserved for the network portion of the address. Class B networks reserve the first two bytes of an IP address for the network address. Class C networks reserve the first three bytes of an IP address for the network address. In all cases, a network manager can decide to use subnetting to assign even more bits to the network portion of the IP address, but never less than the class requires. The following section gives more information on subnetting.

Class A networks have a small number of possible network numbers, but a large number of possible host numbers. Conversely, Class C networks have a small number of possible host numbers, but a large number of possible network numbers. Thus, the InterNIC assigns Class A addresses to large organizations that have very large numbers of IP hosts, while smaller organizations, with fewer hosts, get Class B or Class C addresses. You can tell the various classes apart by the value of the first (or high-order) byte. Class A networks use values from 1 to 127, Class B networks use values from 128 to 191, and Class C networks use values from 192 to 223. The following table summarizes some of the differences between Class A, B, and C networks.

Class	First byte	Number of networks possible per class	Number of hosts possible per network	Format of address (without subnetting)	Example
A	1-127	127	16,777,214	net.host.host.host	97.3.14.250
B	128-191	16,384	65,534	net.net.host.host	140.100.10.11
C	192-223	2,097,152	254	net.net.net.host	197.204.13.7

Subnets and subnet masks

Often an entire organization is assigned only one IP network number. If the organization has several IP networks connected together with IP routers, the network manager can use subnetting to distinguish between these networks, even though they all use the same network number. Each physical network becomes a subnet with a unique subnet number.

Subnet numbers appear within IP addresses, along with network numbers and host numbers. Since an IP address is always 32 bits long, using subnet numbers means either the network number or the host numbers must use fewer bits, in order to leave room for the subnet numbers. Since the InterNIC assigns the network number proper, it should not change, so the subnet numbers must be created out of bits that would otherwise be part of the host numbers.

Subnet masks

To create subnets, the network manager must define a subnet mask, a 32-bit number that indicates which bits in an IP address are used for network and subnetwork addresses, and which are used for host addresses. One subnet mask should apply to all IP networks that are physically connected together and share a single assigned network number. Subnet masks are often written in decimal notation, like IP addresses, but they are most easily understood in binary notation. When a subnet mask is written in binary notation, each numeral 1 indicates that the corresponding bit in the IP address is part of the network or subnet address. Each 0 indicates that the corresponding bit is part of the host address. The following table shows the proper subnet masks to use for each class of network, when no subnets are required.

Class	Subnet mask for a network with no subnets
A	Binary: 11111111.00000000.00000000.00000000 Decimal: 255.0.0.0
B	Binary: 11111111.11111111.00000000.00000000 Decimal: 255.255.0.0
C	Binary: 11111111.11111111.11111111.00000000 Decimal: 255.255.255.0

To know whether subnets are being used or not, you must know what subnet mask is being used—you cannot determine this information simply from an IP address. Subnet mask information is configured as part of the process of setting up IP routers and gateways such as the Netopia R310.

Note: If you receive a routed account from an ISP, there must be a mask associated with your network IP address. By using the IP address with the mask you can discover exactly how many IP host addresses you actually have.

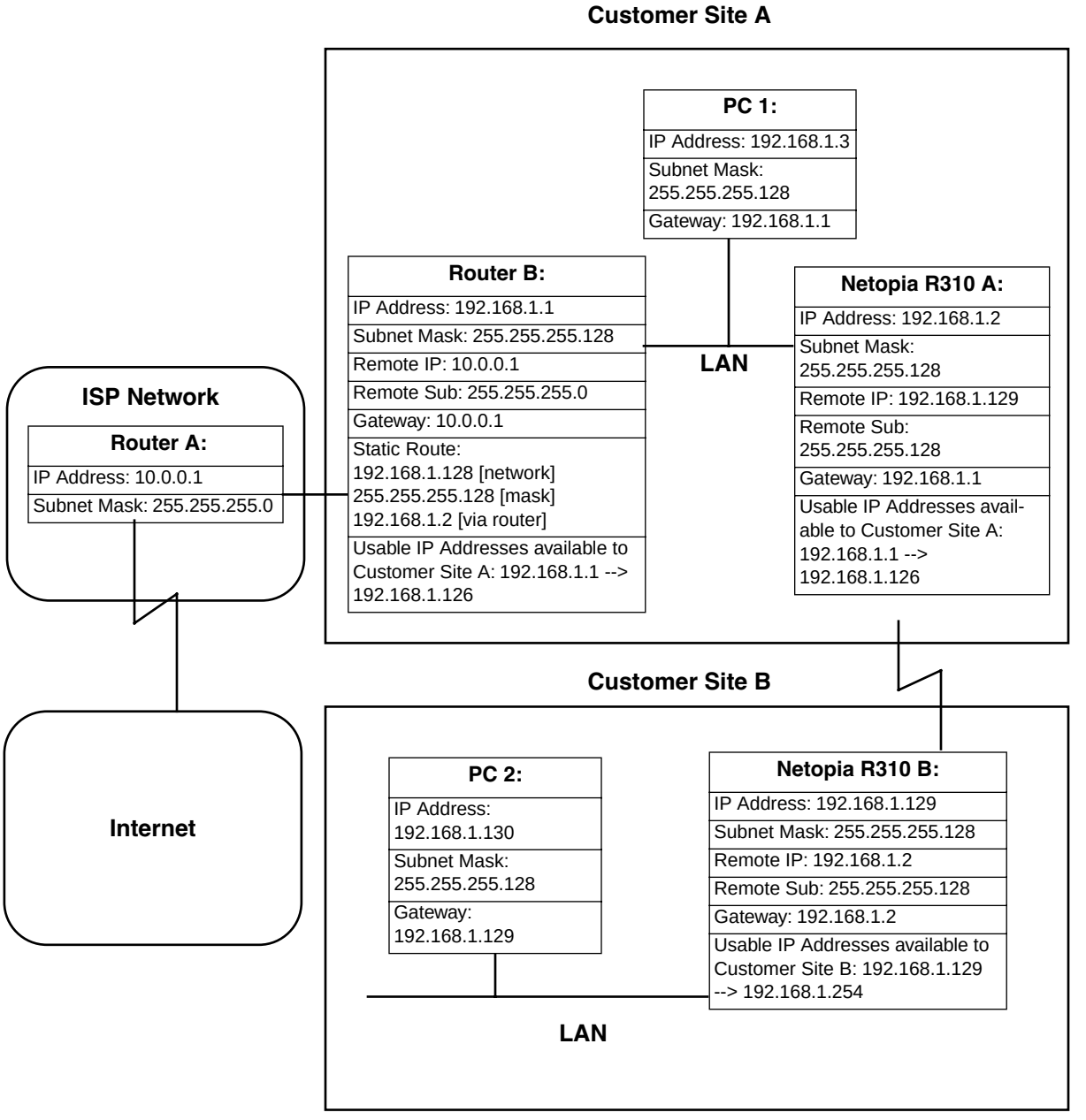
To configure subnets properly, you must also be able to convert between binary notation and decimal notation.

Example: Using subnets on a Class C IP internet

When setting up IP routing with a Class A Address, or even multiple Class C Addresses, subnetting is fairly straightforward. Subnetting a single Class C address between two networks, however, is more complex. This section describes the general procedures for subnetting a single Class C network between two Netopia routers so that each can have Internet access.

Network configuration

Below is a diagram of a simple network configuration. The ISP is providing a Class C address to the customer site, and both networks A and B want to gain Internet access through this address. Netopia R310 B connects to Netopia R310 A and is provided Internet access through Routers A and B.



Background

The IP Addresses and routing configurations for the devices shown in the diagram are outlined below. In addition, each individual field and its meaning are described.

The “IP Address” and “Subnet Mask” fields define the IP Address and Subnet Mask of the device's Ethernet connection to the network while the “Remote IP” and “Remote Sub” fields describe the IP Address and Subnet mask of the remote router. This information is entered in the Connection Profile of the Netopia R310.

The “Gateway” field describes the router or workstation's default gateway or, where they will send their packets if the appropriate route is not known. The “Static Route” field, which is only shown on Router B, tells Router B what path to take to get to the network defined by Netopia R310 B. Finally, the “Usable IP Address” field shows the range of IP Addresses available to the hosts of that network.

Note that the IP Addresses given in this section are for example purposes only. Do not use these addresses when configuring your network.

With this configuration, both Customer Site A and B can gain Internet access through Routers A and B, with no reconfiguration of the ISP's equipment. The most important item in this configuration is the Static Route defined on Router B. This tells Router B what path to take to get to the network defined by Netopia R310 B. Without this information, Customer Site B will be able to access Customer Site A, but not the Internet.

If it is not possible to define a Static Route on Router B, RIP could be enabled to serve the same purpose. To use RIP instead of a Static Route, enable Transmit RIP on Netopia R310 A and Transmit and Receive RIP on Router B. This will allow the route from Customer Site B to propagate on Router B and Customer Site A.

Example: Working with a Class C subnet

Suppose that your organization has a site with only 10 hosts, and no plans to add any new hosts. You don’t need a full Class C address for this site. Many ISPs offer Internet access with only a portion of a full Internet address.

For example, you may obtain the Class C address 199.14.17.48, with the mask 255.255.255.240. From the previous example, you can see that this gives you 14 host addresses to distribute to the hosts at your site. In effect, your existing network of 10 hosts is a subnet of the ISP’s network. Since the Class C address has already been reduced to subnets, you cannot further subnet your network without the risk of creating network routing problems (since you must use the mask issued by the ISP). This, however, is not a problematic limitation for your small network.

The advantages to this situation is the greater ease and lower cost of obtaining a subnet from an ISP rather than a full Class C address.

Distributing IP addresses

To set up a connection to the Internet, you may have obtained a block of IP host addresses from an Internet service provider. When configuring the Netopia R310, you gave one of those addresses to its Ethernet port, leaving a number of addresses to distribute to computers on your network.

There are two schemes for distributing the remaining IP addresses:

- Manually give each computer an address
- Let the Netopia R310 automatically distribute the addresses

These two methods are not mutually exclusive; you can manually issue some of the addresses while the rest are distributed by the Netopia R310. Using the Router in this way allows it to function as an address server.

One reason to use the Netopia R310 as an address server is that it takes less time than manually distributing the addresses. This is particularly true if you have many addresses to distribute. You only need to enter information once, rather than having to repeatedly enter it on each host separately. This also reduces the potential for misconfiguring hosts.

Another reason to use the Netopia R310 as an address server is that it will only distribute addresses to hosts that need to use them.

All Netopia R310s come with an integrated Dynamic Host Control Protocol (DHCP) server. Some routers also come with a Macintosh Internet Protocol (MacIP) server. These servers provide a means of distributing IP addresses to either a Mac or PC workstation as needed.

When setting up the DHCP or MacIP servers in the Netopia R310, it is necessary to understand how workstations lease, renew, and release their IP addresses. This information will be helpful in determining dynamic address allocation for a network.

The term "lease" describes the action of a workstation requesting and using an IP address. The address is dynamic and can be returned to the address pool at a later time.

The term "renew" refers to what the workstations do to keep their leased IP address. At certain intervals, the workstation talks to the DHCP or MacIP server and renews the lease on that IP address. This renewal allows the workstation to keep and use the assigned IP address until the next renewal period.

The term "release" refers to a situation where the workstation is no longer using its assigned IP address or has been shut down. IP addresses can be manually released as well. The IP address goes back into the DHCP or MacIP address pool to be reassigned to another workstation as needed.

Technical note on subnet masking

Note: The IP address supplied by the Netopia R310 will be a unique number. You may wish to replace this number with a number that your ISP supplies if you are configuring the router for a static IP address. The automatic IP mask supplied by SmartStart is a Class C address. However, the Netopia R310 and all devices on the same local network must have the same subnet mask. If you require a different class address, you may edit the IP Mask field to enter the correct address. Refer to the table below.

Number of Devices (other than Netopia R310) on Local Network	Largest Possible Ethernet Subnet Mask
1	255.255.255.252
2-5	255.255.255.248
6-13	255.255.255.240
14-29	255.255.255.224

Number of Devices (other than Netopia R310) on Local Network	Largest Possible Ethernet Subnet Mask
30-61	255.255.255.192
62-125	255.255.255.128
125-259	255.255.255.0

Configuration

This section describes the specific IP address lease, renew, and release mechanisms for both the Mac and PC, with either DHCP or MacIP address serving.

DHCP Address Serving

Windows 95 Workstation:

- The Win95 workstation requests and renews its lease every half hour.
- The Win95 workstation does NOT relinquish its DHCP address lease when the machine is shut down.
- The lease can be manually expired using the WINIPCFG program from the Win95 machine, which is a command line program executable from the DOS prompt or from the START:RUN menu.

Windows 3.1 Workstation (MSTCP Version 3.11a):

- The Win3.1 workstation requests and renews its lease every half hour.
- The Win3.1 workstation does NOT relinquish its DHCP address lease when the user exits Windows and goes to DOS.
- The lease can be manually expired by typing IPCONFIG /RELEASE from a DOS window within Windows or from the DOS prompt.</UL>

Macintosh Workstation (Open Transport Version 1.1 or later):

- The Mac workstation requests and renews its lease every half hour.
- The Mac workstation will relinquish its address upon shutdown in all but one case. If the TCP/IP control panel is set to initialize at start-up, and no IP services are used or the TCP/IP control panel is not opened, the DHCP address will NOT be relinquished upon shutdown. However, if the TCP/IP control panel is opened, or if an IP application is used, the Mac WILL relinquish the lease upon shutdown.
- If the TCP/IP control panel is set to acquire an address only when needed (therefore a TCP/IP application must have been launched to obtain a lease) the Mac WILL relinquish its lease upon shutdown every time.

Netopia R310 DHCP Server Characteristics

- The Netopia R310 ignores any lease-time associated with a DHCP request and automatically issues the DHCP address lease for one hour.
- The Netopia R310 does release the DHCP address back to the available DHCP address pool precisely one hour after the last heard lease request as some other DHCP implementations may hold on to the lease for an additional time after the lease expired, to act as a buffer for variances in clocks between the client and server.

MacIP Serving

Macintosh Workstation (MacTCP or Open Transport):

Once the Mac workstation requests and receives a valid address, the Netopia R310 will actively check for the workstation's existence once every minute.

- For a DYNAMIC address, the Netopia R310 will release the address back to the address pool after it has lost contact with the Mac workstation for over 2 minutes.
- For a STATIC address, the Netopia R310 will release the address back to the address pool after it has lost contact with the Mac workstation for over 20 minutes.

Netopia R310 MacIP Server Characteristics

The Mac workstation uses ATP to both request and receive an address from the Netopia R310's MacIP server. Once acquired, NBP confirm packets will be sent out every minute from the Netopia R310 to the Mac workstation.

Manually distributing IP addresses

If you choose to manually distribute IP addresses, you must enter each computer's address into its TCP/IP stack software. Once you manually issue an address to a computer, it possesses that address until you manually remove it. That's why manually distributed addresses are sometimes called static addresses.

Static addresses are useful in cases when you want to make sure that a host on your network cannot have its address taken away by the address server. A network administrator's computer, a computer dedicated to communicating with the Internet, and routers are appropriate candidates for a static address.

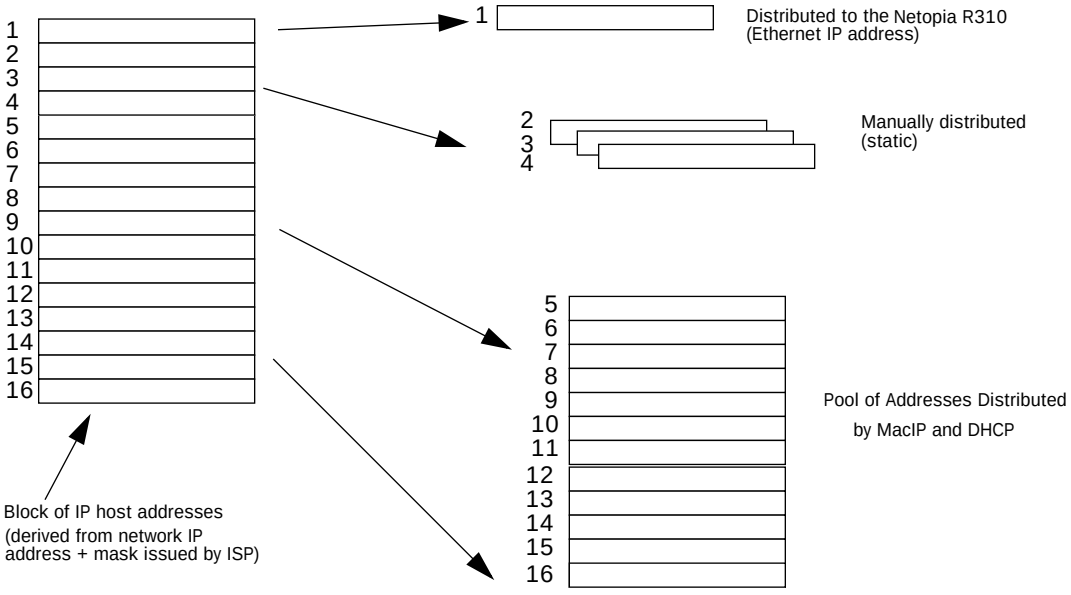
Using address serving

The Netopia R310 provides two ways to serve IP addresses to computers on a network. The first, Dynamic Host Configuration Protocol (DHCP), is supported by PCs with Microsoft Windows and a TCP/IP stack. Macintosh computers using Open Transport and computers using the UNIX operating system may also be able to use DHCP. The second way, MacIP, is for Macintosh computers.

The Netopia R310 can use both DHCP and MacIP. Whether you use one or both will depend on your particular networking environment. If that environment includes both PCs and Macintosh computers that do not use Open Transport, you will need to use both DHCP and MacIP to distribute IP addresses to all of your computers.

Tips and rules for distributing IP addresses

- Before you allocate IP addresses using DHCP and MacIP, consider whether you need to set aside any static addresses.
- Note any planned and currently used static addresses before you use DHCP and MacIP.
- Avoid fragmenting your block of IP addresses. For example, try to use a continuous range for the static addresses you choose.



The figure above shows an example of a block of IP addresses being distributed correctly.

The example follows these rules:

- An IP address must not be used as a static address if it is also in a range of addresses being distributed by DHCP or MacIP.
- A single IP address range is used by all the address-served clients. These include DHCP, BOOTP, MacIP, and WAN clients, even though BOOTP and static MacIP clients might not be considered served.
- The address range specified for address-served clients cannot wrap around from the end of the total available range back to the beginning. See below for a further explanation and an example.
- The network address issued by an ISP cannot be used as a host address.

A DHCP example

Suppose, for example, that your ISP gave your network the IP address 199.1.1.32, and a 4-bit subnet mask. Address 199.1.1.32 is reserved as the network address. Address 199.1.1.47 is reserved as the broadcast address. This leaves 14 addresses to allocate, from 199.1.1.33 through 199.1.1.46. If you want to allocate a sub-block of 10 addresses using DHCP, enter “10” in the DHCP Setup screen’s **Number of Addresses to Allocate** item. Then, in the same screen’s **First Address** item, enter the first address in the sub-block to allocate such that all 10 addresses are within your original block. You could enter 199.1.1.33, or 199.1.1.37, or any address between them. Note that if you entered 199.1.1.42 as the first address, network routing errors would probably result because you would be using a range with addresses that do not belong to your network (199.1.1.49, 199.1.1.50, and 199.1.1.51).

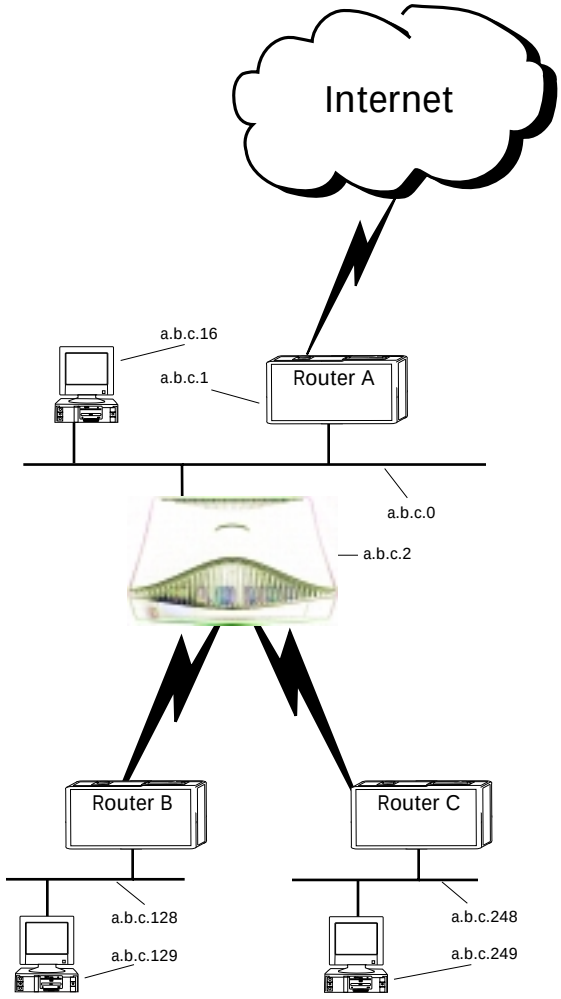
Nested IP subnets

Under certain situations, you may wish to create remote subnets from the limited number of IP addresses issued by your ISP or other authority. You can do this using connection profiles. These subnets can be nested within the range of IP addresses available to your network.

For example, suppose that you obtain the Class C network address a.b.c.0 to be distributed among three networks. This network address can be used on your main network while portions of it can be subnetted to the two remaining networks.

Note: The IP address a.b.c.0 has letters in place of the first three numbers to generalize it for this example.

The figure at left shows a possible network configuration following this scheme. The main network is set up with the Class C address a.b.c.0, and contains Router A (which could be a Netopia R310), a Netopia R310, and a number of other hosts. Router A maintains a link to the Internet, and may be used as the default gateway.



Routers B and C (which could also be Netopia R310s) serve the two remote networks that are subnets of a.b.c.0. The subnetting is accomplished by configuring the Netopia R310 with connection profiles for Routers B and C (see the following table).

Connection profile	Remote IP address	Remote IP mask	Bits available for host address
for Router B	a.b.c.128	255.255.255.192	7
for Router C	a.b.c.248	255.255.255.248	3

The Netopia R310's connection profiles for Routers B and C create entries in its IP routing table. One entry points to the subnet a.b.c.128, while a second entry points to the subnet a.b.c.248. The IP routing table might look similar to the following:

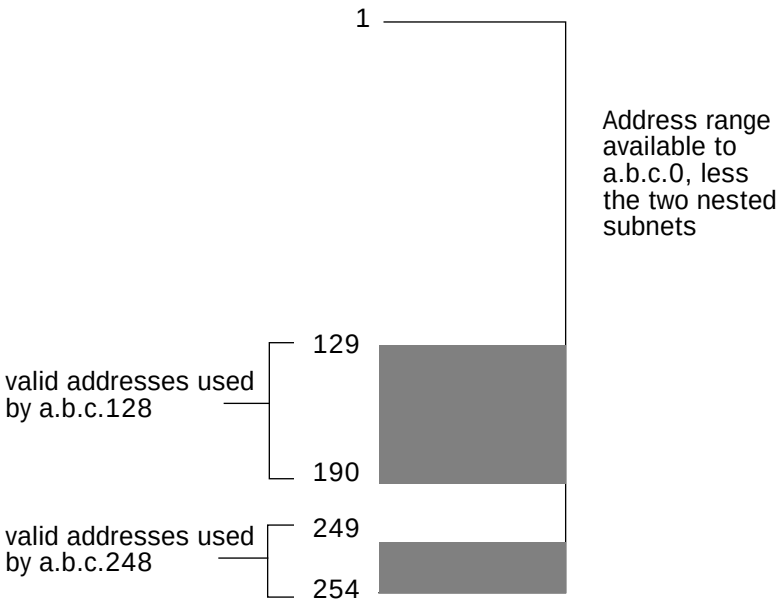
```
                                IP Routing Table

Network Address-Subnet Mask-----via Router------Port--Age--------Type------
-----------------------------------SCROLL UP--------------------------------
0.0.0.0         0.0.0.0         a.b.c.1 WAN     3719              Management
127.0.0.1       255.255.255.255 127.0.0.1 lp1   6423               Local
a.b.c.128       255.255.255.192 a.b.c.128 WAN   5157               Local
a.b.c.248       255.255.255.248 a.b.c.248 WAN   6205               Local


---------------------------------SCROLL DOWN--------------------------------
UPDATE
```

Let's see how a packet from the Internet gets routed to the host with IP address a.b.c.249, which is served by Router C. The packet first arrives at Router A, which delivers it to its local network (a.b.c.0). The packet is then received by the Netopia R310, which examines its destination IP address.

The Netopia R310 compares the packet's destination IP address with the routes in its IP routing table. It begins with the route at the bottom of the list and works up until there's a match or the route to the default gateway is reached.

When a.b.c.249 is masked by the first route's subnet mask, it yields a.b.c.248, which matches the network address in the route. The Netopia R310 uses the connection profile associated with the route to connect to Router C, and then forwards the packet. Router C delivers the packet to the host on its local network.

The following diagram illustrates the IP address space taken up by the two remote IP subnets. You can see from the diagram why the term nested is appropriate for describing these subnets.



Broadcasts

As mentioned earlier, binary IP host or subnet addresses composed entirely of ones or zeros are reserved for broadcasting. A broadcast packet is a packet that is to be delivered to every host on the network, if both the host address and the subnet address are all ones or all zeros, or to every host on the subnetwork, if the host address is all ones or all zeros but the subnet address is a combination or zeros and ones. Instead of making many copies of the packet, individually addressed to different hosts, all the host machines know to pay attention to broadcast packets, as well as to packets addressed to their specific individual host addresses. Depending on the age and type of IP equipment you use, broadcasts will be addressed using either all zeros or all ones, but not both. If your network requires zeros broadcasting, you must configure this through SNMP.

Packet header types

As previously mentioned, IP works with other protocols to allow communication over IP networks. When IP is used on an Ethernet network, IP works with the Ethernet or 802.3 framing standards, among other protocols. These two protocols specify two different ways to organize the very first signals in the sequence of electrical signals that make up an IP packet travelling over Ethernet. By default, the Netopia R310 uses Ethernet packet headers for IP traffic. If your network requires 802.3 IP framing, you must configure this through SNMP.

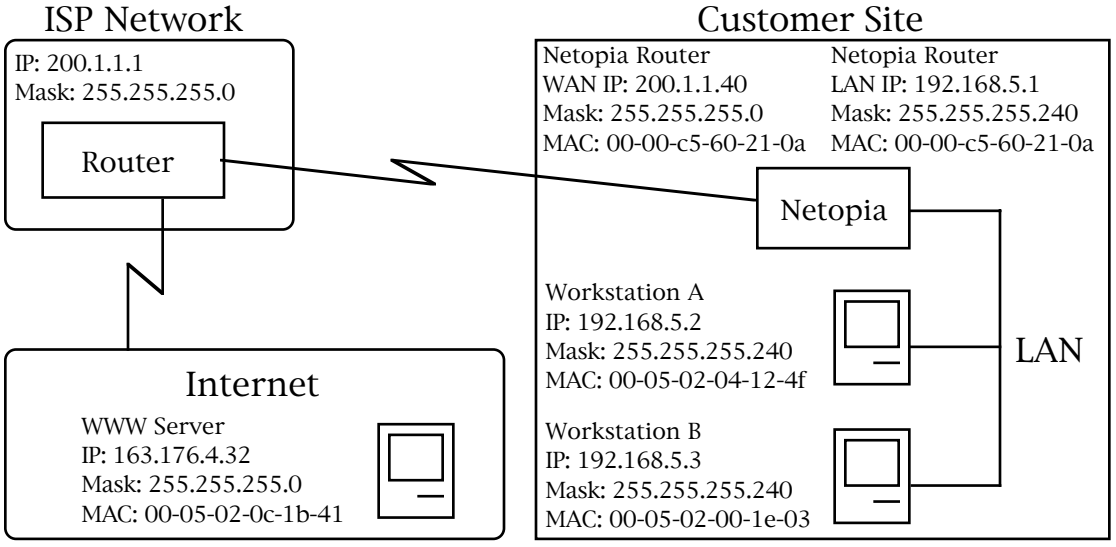
Appendix E

Understanding Netopia NAT Behavior

This appendix describes how Network Address Translation works within the Netopia R310. The Netopia R310 implements a powerful feature called Network Address Translation (NAT) as specified in RFC 1631. NAT is used for IP address conservation and for security purposes since there will only be a single IP "presence" on the WAN. This appendix describes the NAT functionality within the Netopia R310 and provides examples for setup and use.

Network Configuration

Below is a diagram of the network referenced in this appendix.



Background

NAT is a mechanism employed within the Netopia R310 to acquire a statically or dynamically assigned IP address on its WAN interface and proxy against locally assigned IP addresses on its LAN interface. The Netopia R310 uses a one-to-many IP address mapping scheme, that is against a single IP address the Netopia R310 acquires on its WAN interface the Netopia R310 can proxy 14, 30, or an unlimited number of IP hosts on the LAN interface.

In order to fully understand how NAT works you must understand how a PPP connection is established and IP addresses are negotiated.

When the Netopia R310 establishes a connection over its WAN interface with another router it uses the Point to Point Protocol (PPP). Within PPP there is a Network Control Protocol (NCP) called Internet Protocol Control Protocol (IPCP) which handles the negotiation of IP addresses between the two routers, in this case the Netopia R310 at the customer site above and the Router at the Internet Service Provider (ISP).

If the Netopia R310 calls the Router at the ISP with NAT disabled, the Netopia negotiates its LAN interface address (as specified in IP Setup within the Netopia R310's console) with the Router at the ISP through IPCP and then sets up routing. From the previous diagram you can see that the address for the Netopia R310 is 192.168.5.1 and the address of the Router at the ISP is 200.1.1.1. Assuming that the addresses negotiated by the routers are valid and unique for the Internet, the Netopia R310 and the hosts on its LAN would be able to access the Internet.

If the Netopia R310 calls the Router at the ISP with NAT enabled, instead of negotiating the LAN interface address the Netopia R310 suggests the address 0.0.0.0 through IPCP. When the Router at the ISP sees this all-zeros IPCP request, the Router can either pull a free dynamic IP address from its pool and assign it to the Netopia R310's WAN interface or, if configured to do so, match the Netopia R310's incoming connection profile and assign a pre-configured static IP address to the Netopia R310's WAN interface.

From the previous diagram, you can see that the IP address assigned to the Netopia R310's WAN interface is 200.1.1.40, while the IP address assigned to the LAN interface remains the same. The LAN interface address 192.168.5.1 is thus hidden from the ISP and the Internet, and the Netopia R310 only has a single valid IP presence on the Internet. The LAN interface IP address for the Netopia R310 can be any IP address, however it is recommended that you use the IANA specified 192.168.X.X Class C address range which is used for networks not attached to the Internet. This address range is described in RFC 1597.

The dynamic IP address acquisition on the WAN interface of the Netopia R310 is one of several features of NAT. Another is the mapping of locally assigned IP addresses to the single globally unique IP address acquired by the Netopia R310 on its WAN interface. NAT employs several things to accomplish this seamlessly. You must look at the formatting of an IP packet before IP address remapping can be explained.

Every IP packet that is transmitted across the Netopia R310's LAN interface or across the WAN interface to the Internet contains several bits of information that indicate to any device where the packet is going and where it came from. In particular you have the source and destination port and source and destination IP addresses.

A port is used within IP to define a particular type of service and could be either a Transmission Control Protocol (TCP) port or User Datagram Protocol (UDP) port. Both TCP and UDP are protocols that use IP as the underlying transport mechanism. The major difference between TCP and UDP is that TCP is a reliable delivery service whereas UDP is a "best effort" delivery service. A list of well known TCP or UDP ports and services can be found in RFC 1700.

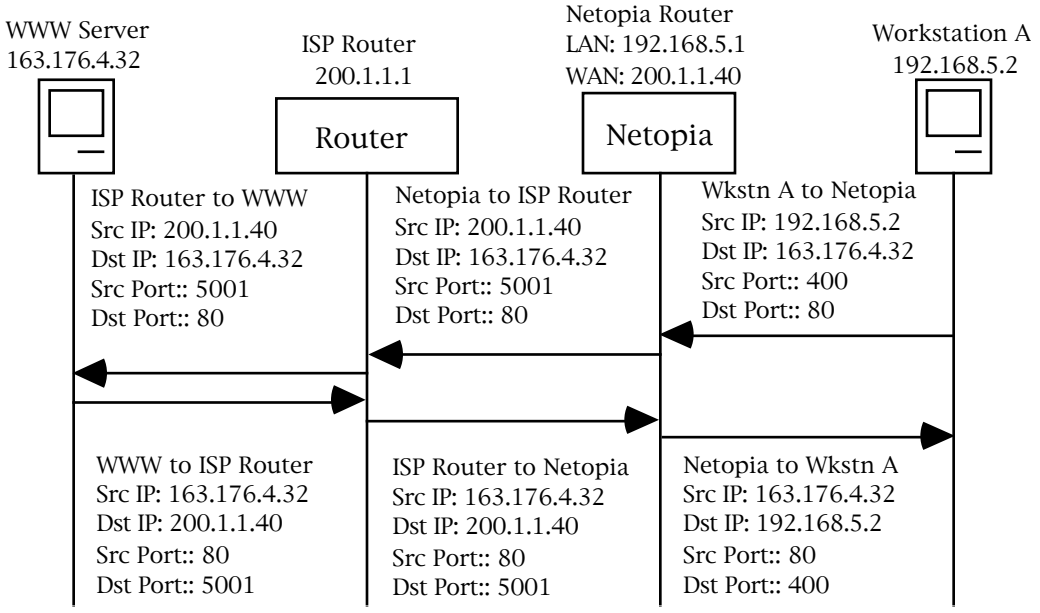
If Workstation A wants to communicate with a World Wide Web (WWW) Server on the Internet and the Netopia R310 does not have NAT enabled, Workstation A forms an IP packet with the source IP address of 192.168.5.2 and destination IP address of 163.176.4.32. The source port could be 400 while the destination port would be 80 (WWW server). The Netopia R310 then looks at this IP packet, determines the best routing method and sends that packet on its way across the WAN interface to the WWW Server on the Internet.

With NAT enabled the Netopia R310 does something different. For example, suppose that Workstation A again wants to communicate with the WWW Server on the Internet. Workstation A forms an IP packet with the source IP address of 192.168.5.2 and destination IP address of 163.176.4.32 and source port could be 400 while the destination port would be 80 (WWW server).

When the Netopia R310 receives this IP packet, it can not simply forward it to the WAN interface and the Internet since the IP addresses on the LAN interface are not valid or globally unique for the Internet. Instead the Netopia R310 has to change the IP packet to reflect the IP address that was acquired on the WAN interface from the ISP.

The Netopia R310 will first substitute the source IP address with the IP address that was acquired on the WAN interface which in this case is 200.1.1.40. Next the Netopia R310 will substitute the source TCP or UDP port with a TCP or UDP port from within a specified range maintained within the Netopia R310. And finally the modified IP packet's checksum is recalculated (as specified in RFC 1631) and the packet is transmitted across the WAN interface to its destination, the WWW Server on the Internet.

If the send and response IP packets were drawn out, this process would look like the following:

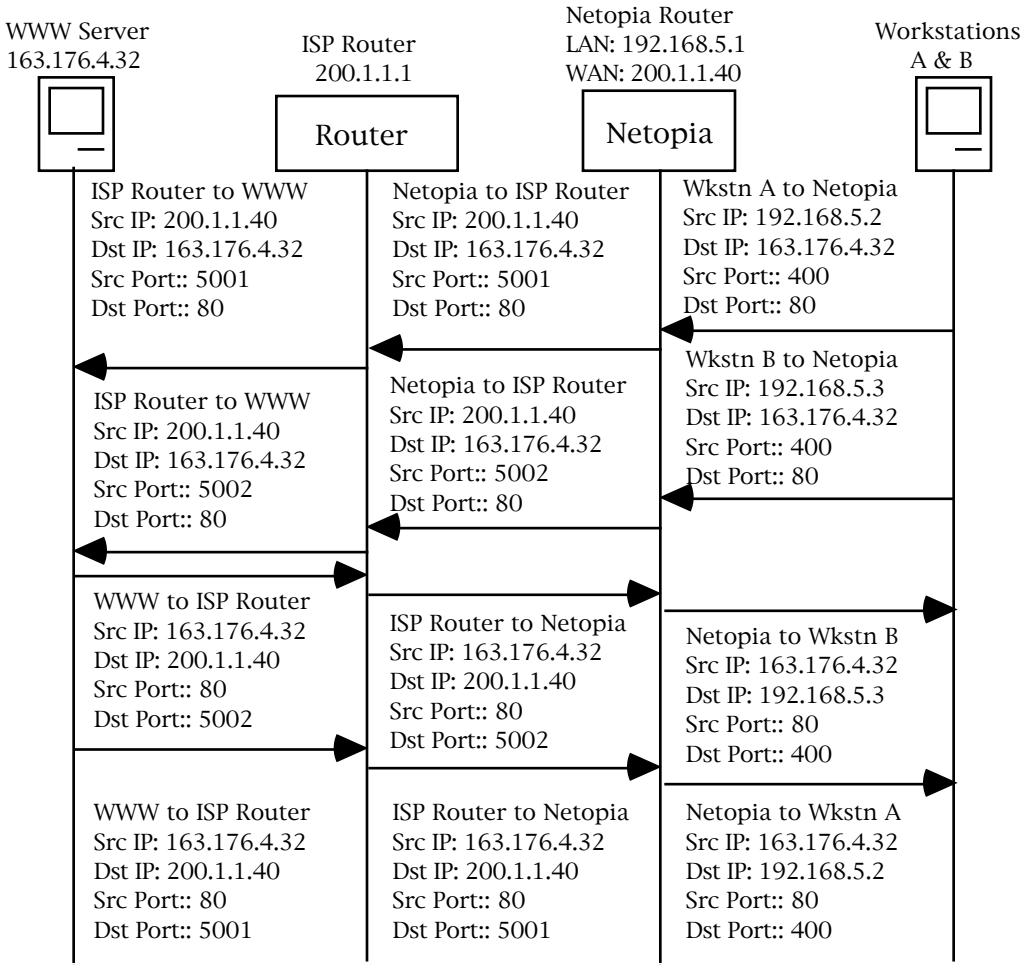


As you can see, the IP packet from Workstation A is sent to the Netopia R310 and the source IP address is substituted with 200.1.1.40 and the source port is substituted with 5001, then the IP packet checksum is recalculated. When this modified packet reaches the WWW Server on the Internet, the WWW Server responds and sends the IP packet back to destination IP address 200.1.1.40 and destination port 5001.

When the Netopia R310 receives this IP packet from the WWW Server, the Netopia R310 replaces the destination IP address with 192.168.5.2, the address for Workstation A. The port is changed back to 400, the IP packet checksum is recalculated, and the IP packet is sent to Workstation A on the Netopia R310s LAN interface.

The reasons for the IP address changes are obvious from the diagram above but what is not so obvious is why the TCP or UDP source ports need to be changed as well. These are changed and maintained in an internal table so the Netopia R310 can determine which host on the local LAN interface sent the IP packet and what host the response from the WAN interface is going to go to on the LAN interface. This becomes especially important when two or more hosts on the LAN interface are accessing the same type of service on the Internet, like a WWW Server (Port 80), for example.

Now look at how two hosts on the LAN interface accessing the same WWW Server on the Internet will work:



As you can see, when Workstation A and Workstation B transmit an IP packet to the WWW Server on the Internet, they have unique source IP addresses on the LAN interface but potentially the same source ports, which in this case is 400. When the Netopia R310 receives these packets, the source IP addresses are substituted with the single globally unique IP address that was acquired on the WAN interface which is 200.1.1.40.

Now both IP packets have the exact same source IP address (200.1.1.40) and source ports (400). The way the Netopia R310 is then able to distinguish between the two IP packets is to change the source TCP or UDP ports and keep this information in an internal table. As seen above, the source port for Workstation A has been changed to 5001 and the source port for Workstation B has been changed to 5002.

If you were to look at the internal port mapping table that is maintained by the Netopia R310, it would look similar to the following:

Source LAN IP	Source LAN Port	Remapped LAN Port
192.168.5.2	TCP 400	TCP 5001
192.168.5.3	TCP 400	TCP 5002

With this information the Netopia R310 can determine the appropriate routing for an IP response from the Internet. In this case when the WWW Server responds with a destination port of 5001, the Netopia R310 can see that this packet's destination on the local LAN interface is actually Workstation A at IP address 192.168.5.2. Likewise with the response for port 5002, the Netopia R310 can see that this packet's destination on the local LAN interface is actually Workstation B at IP address 192.168.5.3.

Exported services

Note that this “automatic” port remapping and IP address substitution only works in one direction, for IP packets that originated on the LAN interface destined to the WAN interface and the Internet. In order for port remapping and IP address substitution to work in the other direction, that is, hosts on the Internet wishing to originate an IP packet destined to a host on the Netopia R310s LAN interface, a manual redirection of TCP or UDP ports as well as destination IP addresses within the Netopia R310 is required. This manual port remapping and IP address substitution is accomplished by setting up Exported Services.

Exported Services are essentially user defined pointers for a particular type of incoming TCP or UDP service from the WAN interface to a host on the local LAN interface. This is necessary since the Netopia R310 and thus the attached local LAN has only one IP presence on the WAN interface and Internet. Exported Services allows the user to redirect one type of service, for example Port 21 (FTP), to a single host on the local LAN interface. This will then allow the Netopia R310 to redirect any packets coming in from the Internet with the defined destination TCP or UDP port of Port 21 (FTP) to be redirected to a host on the local LAN interface.

For example, suppose the WWW Server on the Internet with the IP address of 163.176.4.32 wants to access Workstation B on the Netopia R310s local LAN interface which is operating as an FTP Server. The IP address for Workstation B is 192.168.5.3, which is not a valid IP address and thus the WWW Server on the Internet can not use this IP address to access Workstation B.

The WWW Server on the Internet would then have to use the single valid IP address that was acquired on the Netopia R310's WAN interface to access any host on the Netopia R310's local LAN interface, since this is the only valid address for the Internet. But if the WWW Server on the Internet opens a connection to 200.1.1.40 via Port 21 (FTP) and no Exported Services are defined on the Netopia R310, the Netopia R310 will discard the incoming packet since the Netopia R310 itself does not perform the requested service.

Thus you can see why Exported Services are necessary. In the example above, an Exported Service needs to be defined within the Netopia R310 redirecting any incoming IP traffic with a destination port of 21 to the host on the local LAN interface with the IP address of 192.168.5.3.

If the WWW Server on the Internet then tries to open a connection to the IP address of 200.1.1.40 with the appropriate Exported Service defined, the Netopia R310 will look at the destination port and will find that it is destined for Port 21 (FTP). The Netopia R310 then looks at the internal user-defined Exported Services table and finds that any incoming IP traffic from the WAN port with a destination of Port 21 (FTP) should be redirected to the IP address of 192.168.5.3 on the local LAN interface, which in this case is Workstation B.

Once the appropriate Exported Services are defined, there can be seamless communication between a host on the Internet and a host on the Netopia R310's local LAN interface.

Important notes

Even with the advantages of NAT, there are several things you should note carefully:

- There is no formally agreed upon method among router vendors to handle an all-zeros IPCP request. The majority of router vendors use the all-zeros IPCP request to determine when a dial-in host wants to be assigned an IP address. Some vendors however attempt to negotiate and establish routing with an all-zeros IP address. The Netopia R310 will not allow routing to be established with an all-zeros IP address and the call will be dropped with an error logged in the Device Event History.
- When using NAT it is most likely that the Netopia R310 will be receiving an IP address from a "pool" of dynamic IP addresses at the ISP. This means that the Netopia R310's IP presence on the Internet will change with each connection. This can potentially cause problems with devices on the Internet attempting to access services like WWW and FTP servers on the Netopia R310's local LAN interface. In this case, if a dynamic IP address is assigned to the WAN interface of the Netopia R310 each time, the administrator of the Netopia R310 will have to notify clients wishing to access services on the Netopia R310's LAN interface of the new IP address after each connection.
- With NAT enabled, there cannot be two or more of the same types of service accessible from the Internet on the LAN interface of the Netopia R310. For example, there cannot be multiple FTP servers (Port 23) on the Netopia R310's LAN interface that can be accessible by workstations on the Internet. This is due to the fact that within the Netopia R310 and IP there is no way to distinguish between multiple servers using the same port, in this case port 23.
- Fictional IP addresses may be assigned on the Netopia R310's LAN interface. It is strongly recommended that for the Netopia R310's LAN interface, an IP address from the Class C address range of 192.168.X.X be used. This is because this range is defined by the IANA as an address space that will never be routed through the Internet and is to be used by private Intranets not attached to the Internet.

  If the address range of 192.168.X.X is not used and another range of addresses such as 100.1.1.X is used instead, this address space can potentially overlap an address space that is owned by a user attached to the Internet. Thus if a user on the Netopia R310's LAN interface has an IP address of 100.1.1.2 while the Netopia R310's LAN interface is 100.1.1.2 and the local host wishes to access a host on the Internet with the address of 100.1.1.8, the Netopia R310 has no way of knowing that the 200.1.1.8 address is actually on the Internet and not on its local LAN interface, as the local LAN interface is assigned the IP address range of 200.1.1.1 to 200.1.1.14.

Configuration

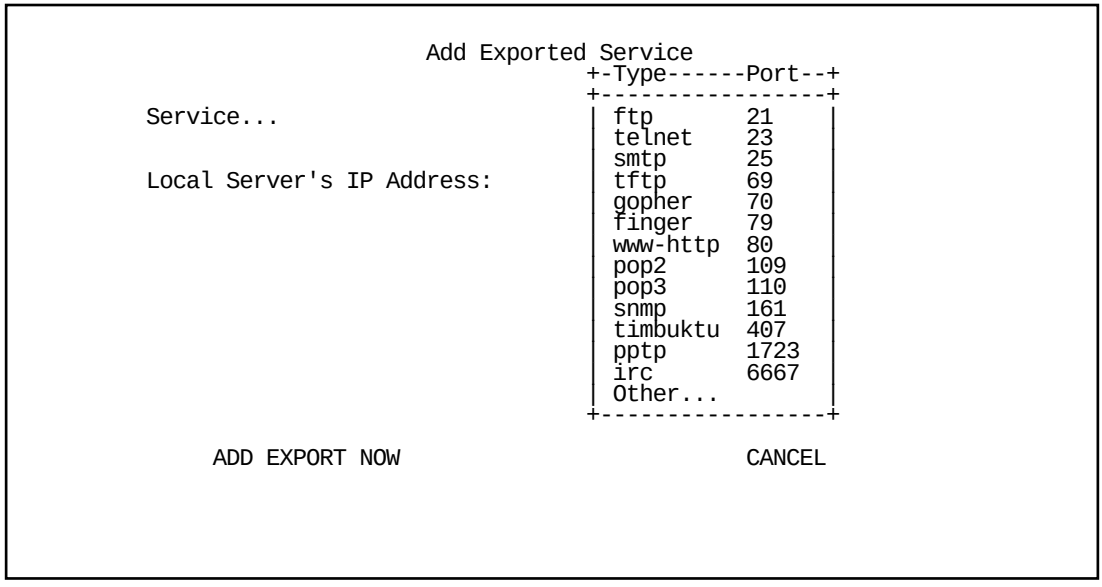
Network Address Translation is enabled by default with the SmartStart configuration utility. You can toggle **Enable Address Translation** to NO or YES in the Connection Profile screen in System Configuration under the IP Profile Parameters section. NAT is enabled on a per-profile basis, so it is possible to have any combination of NAT and non-NAT profiles. An example of enabling NAT is as follows:

```
                        IP Profile Parameters

        Remote IP Address:                 127.0.0.2
        Remote IP Mask:                    255.255.255.0

        Address Translation Enabled:       Yes

        Filter Set...
        Remove Filter Set

        Receive RIP:                       No









Enter the remote IP network's IP address (form xxx.xxx.xxx.xxx decimal).
Configure IP requirements for a remote network connection here.
```

Toggling Address Translation Enabled to Yes enables the Netopia R310 to send out an all-zeros IPCP address that requests an IP to be assigned to the Netopia R310's WAN interface. Note that the remote IP address is 127.0.0.2, which should also be the Default Gateway under IP Setup in System Configuration. This is done for profile matching purposes and because the IP address of the router the Netopia R310 is dialing is not always known.

As mentioned earlier in this appendix, NAT works well for IP sessions originated on the Netopia R310's LAN interface destined for the Internet without any additional configuration. For incoming IP connections from the Internet to a host on the Netopia R310's LAN interface, Exported Services need to be used.

Exported Services are configured under IP Setup in System Configuration. This is where a particular type of TCP or UDP service originating from the Internet is redirected to a host on the Netopia R310's LAN interface. An example of this screen is as follows:



Within Exported Services is a pop-up containing a list of well known TCP and UDP services that can be redirected to a single host on the Netopia R310's LAN interface. There is also an "Other..." option which allows for manual configuration of additional TCP or UDP ports. There can be a total of 32 Exported Services that can be defined.

When a particular type of service is redirected to an IP address, that service is removed from the pop-up list, since only one type of service can be redirected to a single host. However several different types of services can be redirected to a single or multiple hosts. For example, port 80 (WWW Server) could be redirected to 192.168.5.3 on the Netopia R310's LAN interface as well as port 23 (Telnet) can be redirected to that same host.

Summary

NAT is a powerful feature of the Netopia R310 and when used and set up properly can yield a secure network while only using one IP address on the WAN interface. Note that the addresses listed in this appendix are for demonstration purposes only. Do not use these addresses when configuring your local network.

Appendix F

Event Histories

This appendix is a list of some of the events that can appear in the Netopia R310's Event Histories. The text that appears in a history is shown in bold, followed by a brief explanation and the parameters associated with the event. The Event Histories display events for the Device and for the WAN under separate sections.

You can display more information about any event by selecting it in the Event History and pressing Return. See the example Device Event History shown below.

```
                          Device Event History

                                        Current Date --   6/4/97 09:23:53 AM
-Date-----Time-----Event-----------------------------------------------------
---------------------------------SCROLL UP-------------------------------------
06/04/97 08:56:06   IP address server initialization complete
06/04/97 08:56:06 --BOOT: Cold start----------------------------------------
--------------------------------SCROLL DOWN------------------------------------

Return/Enter on event item for details or 'SCROLL [UP/DOWN]' item for scrolling.
```

For example, if you select the BOOT event that occurred at 08:56:06 and press Return, the following popup screen appears:

```
          +-----------------------EVENT DETAILS-----------------------+
          +-----------------------------------------------------------+
          |                                                           |
          | 08:56:06 on Wednesday, June 4, 1997                       |
          | --BOOT: Cold start-----------------------------------------|
          |                  RETURN TO PREVIOUS MENU                  |
          |                                                           |
          |                                                           |
          +-----------------------------------------------------------+
```

ISDN events

ISDN Port Init: ISDN port has been initialized.

ISDN Line Active: ISDN L1 active - L1 not ready to carry L2 data. Associated parameter: switch type or protocol.

ISDN Line Deactivated: ISDN L1 not active - L1 not ready to carry L2 data. Associated parameter: switch type or protocol.

Received Clear Confirmation for our DN: Received clear confirmation from switch. Associated parameter: called directory number.

Received Clear Ind. from DN: Received clear indication from switch. Associated parameter: called directory number. Secondary associated parameter: cause code.

Connection Confirmed to our DN: Received connect confirmation for Connect Request sent to the switch. Associated parameter: called directory number.

Received Connect Ind. for DN: Received connect indication for Call Request sent to the switch. Associated parameter: called directory number.

Received Disc. Ind. from DN: Received disconnect indication from switch. Associated parameter: called directory number. Secondary associated parameter: cause code.

Received Setup Ind. from DN: Received call indication from switch. Associated parameter: called directory number.

Issued Setup Request from our DN: Call request was sent to switch. Associated parameter: called directory number.

Requested Connect to our DN: Connect request for the received call was sent to the switch. Associated parameter: called directory number.

Issued Clear Request for our DN: Clear request was sent to the switch. Associated parameter: called directory number.

Issued Clear Response to DN: Clear response was sent to the switch. Associated parameter: called directory number.

Disconnect Reqested: Disconnect request was sent to switch. Associated parameter: called directory number. Secondary associated parameter: cause code.

ISDN event cause codes

These codes appear as associated (secondary) parameters in some of the ISDN events.

Cause No. 1: unallocated (unassigned number). This cause indicates that the destination requested by the calling user cannot be reached because, although the number is in a valid format, it is not currently assigned (allocated).

Cause No. 2: no route to specified transit network. This cause indicates that the equipment sending this cause has received a request to route the call through a particular transit network which it does not recognize. The equipment sending this cause does not recognize the transit network either because the transit network does not exist or because that particular network, while it does exist, does not serve the equipment that is sending this cause.

This cause is supported on a network-dependent basis.

Cause No. 3: no route to destination. This cause indicates that the called user cannot be reached because the network through which the call has been routed does not serve the destination desired.

This cause is supported on a network-dependent basis.

Cause No. 6: channel unacceptable. This cause indicates that the channel used in this call is not acceptable to the sending entity.

Cause No.7: call awarded and being delivered in an established channel. This cause indicates that the user is receiving an incoming call, which is being connected to a channel already used by that user for similar calls (e.g., packet-mode X.25 virtual calls).

Cause No. 16: normal call clearing. This cause indicates that the call is being cleared because one of the users involved in the call has requested that the call be cleared.

Under normal situations, the source of this cause is not the network.

Cause No. 17: user busy. This cause is used when the called user has indicated the inability to accept another call.

It is noted that the user equipment is compatible with call.

Cause No. 18: no user responding. This cause is used when a user does not respond to a call establishment message with either an alerting or connect indication within the prescribed period of time allocated (defined in Recommendation Q.931 by the expiry of either timer T303 or T310).

Cause No. 19: no answer from user (user alerted). This cause is used when a user has provided an alerting indication but has not provided a connect indication within a prescribed period of time.

This cause is not necessarily generated by Q.931 procedures but may be generated by internal network timers.

Cause No. 21: call rejected. This cause indicates that the equipment sending this cause does not wish to accept this call, although it could have accepted the call because the equipment sending this cause is neither busy nor incompatible.

Cause No. 22: number changed. This cause is returned to a calling user when the called party number indicated by the calling user is no longer assigned. The new called party number may optionally be included in the diagnostic field. If a network does not support this capability, cause No. 1, unassigned (unallocated) number, shall be used.

Cause No. 26: non-selected user clearing. This cause indicates that the specified user has not been awarded the incoming call.

Cause No. 27: destination out of order. This cause indicates that the destination indicated by the user cannot be reached because the interface to the destination is not functioning correctly. The term "not functioning correctly" indicates that a signaling message was unable to be delivered to the remote user: e.g., a physical layer or data link layer failure at the remote user, user equipment off-line, etc.

Cause No. 28: invalid number format (address incomplete). This cause indicates that the called user cannot be reached because the called party number is not a valid format or is not complete.

Cause No. 29: facility rejected. This cause is returned when a facility requested by the user cannot be provided by the network.

Cause No. 30: response to STATUS INQUIRY. This cause is included in the STATUS message when the reason for generated the STATUS message was the prior receive of a STATUS INQUIRY message.

Cause No. 31: normal, unspecified. This cause is used to report a normal even only when no other cause in the normal class applies.

Cause No. 34: no circuit/channel available. This cause indicates that there is no appropriate circuit/channel presently available to handle the call.

Cause No. 38: network out of order. This cause indicates that the network is not functioning correctly and that the condition is likely to last a relatively long period of time: e.g., immediately reattempting the call is not likely to be successful.

Cause No. 41: temporary failure. This cause indicates that the network is not functioning correctly and that the condition is not likely to last a long period of time: e.g., the user may wish to try another call attempt almost immediately.

Cause No. 42: switching equipment congestion. This cause indicates that the switching equipment generating this cause is experiencing a period of high traffic.

Cause No. 43: access information discarded. This cause indicates that the network could not deliver access information to the remote user as requested: i.e., user-to-user information, low layer compatibility, high layer compatibility, or a sub-address as indicated in the diagnostic.

It is noted that the particular type of access information discarded is optionally included in the diagnostic.

Cause No. 44: requested circuit/channel not available. This cause is returned when the circuit or channel indicated by the requesting entity cannot be provided by the other side of the interface.

Cause No. 47: resource unavailable, unspecified. This cause is used to report a resource unavailable event only when no other cause in the resource unavailable class applies.

Cause No 49: Quality of Service not available. This cause is used to report that the requested Quality of Service, as defined in Recommendation X.213, cannot be provided (e.g., throughput or transit delay cannot be supported).

Cause No. 50: requested facility not subscribed. This cause indicates that the requested supplementary service could not be provided by the network because the user has not completed the necessary administrative arrangements with its supporting networks.

Cause No 57: bearer capability not authorized. This cause indicates that the user has requested a bearer capability implemented by the equipment that generated this cause that the user is not authorized to use.

Cause No. 58: bearer capability not presently available. This cause indicates that the user has requested a bearer capability implemented by the equipment that generated this cause which is not available at this time.

Cause No 63: service or option not available, unspecified. This cause is used to report a service or option not available event only when no other cause in the service or option not available class applies.

Cause No. 65: bearer capability not implemented. This cause indicates that the equipment sending this cause does not support the bearer capability requested.

Cause No. 66: channel type not implemented. This cause indicates that the equipment sending this cause does not support the channel type requested.

Cause No. 69: requested facility not implemented. This cause indicates that the equipment sending this cause does not support the requested supplementary service.

Cause No. 70: only restricted digital information bearer capability is available. This cause indicates that a device has requested an unrestricted bearer service but the equipment sending this cause only supports the restricted version of the requested bearer capability.

Cause No. 79: service or option not implemented, unspecified. This cause is used to report a service or option not implemented event only when no other cause in the service or option not implemented class applies.

Cause No. 81: invalid call reference value. This cause indicates that the equipment sending this cause has received a message with a call reference which is not currently in use on the user-network interface.

Cause No. 82: identified channel does not exist. This cause indicates that the equipment sending this cause has received a request to use a channel not activated on the interface for a call. For example, if a user has subscribed to those channels on a primary rate interface numbered from 1 to 12 and the user equipment or the network attempts to use channels 13 through 23, this cause is generated.

Cause No. 83: a suspended call exists, but this call identify does not. This cause indicates that a call resume has been attempted with a call identity which differs from that in use for any presently suspended call(s).

Cause No. 84: call identity in use. This cause indicates that the network has received a call suspend request. The call suspend request contained a call identity (including the null call identity) which is already in use for a suspended call within the domain of interfaces over which the call might be resumed.

Cause No. 85: no call suspended. This call indicates that the network has received a call resume request. The call resume request contained a call identity information element that presently does not indicate any suspended call within the domain interfaces over which calls may be resumed.

Cause No. 86: call having the requested call identity has been cleared. This cause indicates that the network has received a call resume request. The call resume request contained a call identity information element that once indicated a suspended call; however, that suspended call was cleared while suspended (either by network timeout or by remote user).

Cause No. 88: incompatible destination. This cause indicates that the equipment sending this cause has received a request to establish a call that has a low layer compatibility, high layer compatibility, or other compatibility attributes (e.g., data rate) that cannot be accommodated.

Cause No. 91: invalid transit network selection. This cause indicates that a transit network identification of an incorrect format as defined in Annex C/Q.931 was received.

Cause No. 95: invalid message, unspecified. This cause is used to report an invalid message event only when no other cause in the invalid message class applies.

Cause No. 96: mandatory information element is missing. This cause indicates that the equipment sending this cause has received a message that is missing an information element that must be present in the message before that message can be processed.

Cause No. 97: message type non-existent or not implemented. This cause indicates that the equipment sending this cause has received a message with a message type it does not recognize either because this is a message not defined or defined but not implemented by the equipment sending this cause.

Cause No. 98: message not compatible with call state or message type non-existent or not implemented. This cause indicates that the equipment sending this cause has received a message such that the procedures do not indicate that this is a permissible message to receive while in the call state, or a STATUS message was received indicating an incompatible call state.

Cause No. 99: information element non-existent or not implemented. This cause indicates that the equipment sending this cause has received a message that includes information elements not recognized because the information element identifier is not defined or it is defined but not implemented by the equipment sending the cause. However, the information element is not required to be present in the message in order for the equipment sending the cause to process the message.

Cause No. 100: invalid information element contents. This cause indicates that the equipment sending this cause has received an information element which it has implemented; however, one or more of the fields in the information element are coded in a way that has not been implemented by the equipment sending this cause.

Cause No 101: message not compatible with call state. This cause indicates that a message has been received that is incompatible with the call state.

Cause No. 102: recovery on timer expiry. This cause indicates that a procedure has been initiated by the expiry of a timer in association with Q.931 error handling procedures.

Cause No. 111: protocol error, unspecified. This cause is used to report a protocol error event only when no other cause in the protocol error class applies.

Cause No. 127: interworking, unspecified. This cause indicates there has been interworking with a network that does not provide causes for actions it takes; thus, the precise cause for a message being sent cannot be ascertained.

Appendix G

ISDN Configuration Guide

This appendix contains supplemental ISDN configuration information.

This section covers the following topics:

Definitions

The following terms are used in this appendix:

Directory number: The actual phone number associated with the ISDN line you order. Depending on the type of switch protocol used on your line, there may be one directory number for both B-channels, or one for each B-channel.

If you encounter other unfamiliar terms, check the glossary.

Dynamic B-channel usage

If the **B-Channel Usage** item in a connection profile's PPP/MP Options screen is set to **Dynamic** or **2 B, Pre-emptible**, one or both B channels may be in use at any time during a call made with that connection profile. Use of the second B-channel depends on traffic volume.

In addition, one of the B-channels may be relinquished if there is an incoming call, or if a second outgoing connection is made using another connection profile.

The ability to allow incoming calls when both B-channels are in use depends on the type of switch protocol on the local ISDN line, and how that line is provisioned (configured). Some types of switch protocols never allow incoming calls when both B-channels are in use. Switch protocols that do allow incoming calls must have the additional call offering (ACO) parameter turned on for data. ACO for data is off by default.

To find out if your switch protocol supports ACO, or to turn ACO on, contact your ISDN service provider.

Other incoming call restrictions

A B-channel will not be relinquished to admit an incoming call if a connection profile has **B-Channel Usage** set to **2 B-Channels**.

A B-channel will not be relinquished to admit an incoming call when there are two separate concurrent calls. Incoming calls are automatically allowed in when there is at least one B-channel free.

Appendix H

Binary Conversion Table

This table is provided to help you choose subnet numbers and host numbers for IP and MacIP networks that use subnetting for IP addresses.

Decimal	Binary	Decimal	Binary	Decimal	Binary	Decimal	Binary
0	0	32	100000	64	1000000	96	1100000
1	1	33	1000001	65	1000001	97	1100001
2	10	34	100010	66	1000010	98	1100010
3	11	35	100011	67	1000011	99	1100011
4	100	36	100100	68	1000100	100	1100100
5	101	37	100101	69	1000101	101	1100101
6	110	38	100110	70	1000110	102	1100110
7	111	39	100111	71	1000111	103	1100111
8	1000	40	101000	72	1001000	104	1101000
9	1001	41	101001	73	1001001	105	1101001
10	1010	42	101010	74	1001010	106	1101010
11	1011	43	101011	75	1001011	107	1101011
12	1100	44	101100	76	1001100	108	1101100
13	1101	45	101101	77	1001101	109	1101101
14	1110	46	101110	78	1001110	110	1101110
15	1111	47	101111	79	1001111	111	1101111
16	10000	48	110000	80	1010000	112	1110000
17	10001	49	110001	81	1010001	113	1110001
18	10010	50	110010	82	1010010	114	1110010
19	10011	51	110011	83	1010011	115	1110011
20	10100	52	110100	84	1010100	116	1110100
21	10101	53	110101	85	1010101	117	1110101
22	10110	54	110110	86	1010110	118	1110110
23	10111	55	110111	87	1010111	119	1110111
24	11000	56	111000	88	1011000	120	1111000
25	11001	57	111001	89	1011001	121	1111001
26	11010	58	111010	90	1011010	122	1111010
27	11011	59	111011	91	1011011	123	1111011
28	11100	60	111100	92	1011100	124	1111100
29	11101	61	111101	93	1011101	125	1111101
30	11110	62	111110	94	1011110	126	1111110
31	11111	63	111111	95	1011111	127	1111111

Decimal	Binary	Decimal	Binary	Decimal	Binary	Decimal	Binary
128	10000000	160	10100000	192	11000000	224	11100000
129	10000001	161	10100001	193	11000001	225	11100001
130	10000010	162	10100010	194	11000010	226	11100010
131	10000011	163	10100011	195	11000011	227	11100011
132	10000100	164	10100100	196	11000100	228	11100100
133	10000101	165	10100101	197	11000101	229	11100101
134	10000110	166	10100110	198	11000110	230	11100110
135	10000111	167	10100111	199	11000111	231	11100111
136	10001000	168	10101000	200	11001000	232	11101000
137	10001001	169	10101001	201	11001001	233	11101001
138	10001010	170	10101010	202	11001010	234	11101010
139	10001011	171	10101011	203	11001011	235	11101011
140	10001100	172	10101100	204	11001100	236	11101100
141	10001101	173	10101101	205	11001101	237	11101101
142	10001110	174	10101110	206	11001110	238	11101110
143	10001111	175	10101111	207	11001111	239	11101111
144	10010000	176	10110000	208	11010000	240	11110000
145	10010001	177	10110001	209	11010001	241	11110001
146	10010010	178	10110010	210	11010010	242	11110010
147	10010011	179	10110011	211	11010011	243	11110011
148	10010100	180	10110100	212	11010100	244	11110100
149	10010101	181	10110101	213	11010101	245	11110101
150	10010110	182	10110110	214	11010110	246	11110110
151	10010111	183	10110111	215	11010111	247	11110111
152	10011000	184	10111000	216	11011000	248	11111000
153	10011001	185	10111001	217	11011001	249	11111001
154	10011010	186	10111010	218	11011010	250	11111010
155	10011011	187	10111011	219	11011011	251	11111011
156	10011100	188	10111100	220	11011100	252	11111100
157	10011101	189	10111101	221	11011101	253	11111101
158	10011110	190	10111110	222	11011110	254	11111110
159	10011111	191	10111111	223	11011111	255	11111111

Appendix I

Technical Specifications and Safety Information

Description

Dimensions: 124.0 cm (w) x 20.0 cm (d) x 5.3 cm (h)
9.4” (w) x 7.9” (d) x 2.1” (h)

Communications interfaces: The Netopia R310 ISDN Router has an RJ-45 jack for ISDN connections; a 4-port 10Base-T Ethernet hub for your LAN connection; and a DB-9 Console port.

Power requirements

- 12 VDC input
- 1.5 Amps

Environment

Operating temperature: 0° to +40° C

Storage temperature: 0° to +70° C

Relative storage humidity: 20 to 80% non-condensing

Software and protocols

Software media: Software preloaded on internal flash memory; field upgrades done via download to internal flash memory via XMODEM or TFTP

Routing: TCP/IP Internet Protocol Suite, RIP

WAN support: PPP, MP, HDLC

Security: PAP, CHAP, PAP-TOKEN, CACHE-TOKEN, callback, SecurID, IP firewalls, UI password security, and CallerID

SNMP network management: SNMPv1, MIB-II (RFC 1213), Interface MIB (RFC 1229), Ethernet MIB (RFC 1643), Netopia R310 MIB

Management/configuration methods: HTTP (web server), serial console, remote modem console, telnet, SNMP

Diagnostics: PING, event logging, routing table displays, traceroute, statistics counters, Call Accounting

Agency approvals

North America

Safety Approvals:

- United States – UL: 1950 Third Edition
- Canada – CSA: CAN/CSA-C22.2 No. 950-95

EMI:

- FCC Class A

International

Safety Approvals:

- Low Voltage (European directive) 72/23
- EN60950 (Europe)
- ETSI 300 047 (Europe)
- AS/NRZ 3260 (Australia)
- TS001(Australia)
- TS008 (Australia)

EMI Compatibility:

- 89/336/EEC (European directive)
- EN55022:1994 CISPR22 Class B
- EN550082-1:1992 (Immunity)

Network Homologation:

- Telecom Terminal Equipment, 91/263/EEC (European directive): CTR3
- TS031 (Australia)

Regulatory notices

Warning

This is a Class A product. In a domestic environment this product may cause radio interference, in which case the user may be required to take adequate measures. Adequate measures include increasing the physical distance between this product and other electrical devices.

United States. This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC Requirements, Part 68. The Federal Communications Commission (FCC) has established Rules which permit this device to be directly connected to the telephone network. Standardized jacks are used for these connections. This equipment should not be used on party lines or coin phones.

If this device is malfunctioning, it may also be causing harm to the telephone network; this device should be disconnected until the source of the problem can be determined and until repair has been made. If this is not done, the telephone company may temporarily disconnect service.

The telephone company may make changes in its technical operations and procedures; if such changes affect the compatibility or use of this device, the telephone company is required to give adequate notice of the changes. You will be advised of your right to file a complaint with the FCC.

If the telephone company requests information on what equipment is connected to their lines, inform them of:

a) The telephone number to which this unit is connected.

b) The ringer equivalence number

c) The USOC jack required. (RJ11C)

d) The FCC Registration Number. (14 digits provided by FCC)

Items (b) and (d) are indicated on the label. The Ringer Equivalence Number (REN) is used to determine how many devices can be connected to your telephone line. In most areas, the sum of the REN's of all devices on any one line should not exceed five (5.0). If too many devices are attached, they many not ring properly.

Service Requirements. In the event of equipment malfunction, all repairs should be performed by our Company or an authorized agent. Under FCC rules, no customer is authorized to repair this equipment. This restriction applies regardless of whether the equipment is in or our of warranty. It is the responsibility of users requiring service to report the need for service to our Company or to one of our authorized agents. Service can be obtained at Netopia, Inc., 2470 Mariner Square Loop, Alameda, California, 94501.

Important

This product was tested for FCC compliance under conditions that included the use of shielded cables and connectors between system components. Changes or modifications to this product not authorized by the manufacturer could void your authority to operate the equipment.

Canada. This digital apparatus does not exceed the Class A limits for radio noise emission from digital apparatus set out in the Radio Interference Regulations of the Canadian Department of Communications.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la classe A prescrites dans le Réglement sur le brouillage radioélectrique édicté par le ministère des Communications du Canada.

Declaration for Canadian users

The Canadian Industry Canada label identifies certified equipment. This certification means that the equipment meets certain telecommunications network protective, operation and safety requirements. The Department does not guarantee the equipment will operate to the user's satisfaction.

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. In some cases, the company's inside wiring associated with a single line individual service may be extended by means of a certified connector assembly (telephone extension cord.) The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to the certified equipment should be made by an authorized Canadian maintenance facility designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

Users should ensure for their own protection that the electrical ground connections of the power utility, telephone lines and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

Caution

Users should not attempt to make such connections themselves, but should contact the appropriate electric inspection authority, or electrician, as appropriate.

The Load Number (LN) assigned to each terminal device denotes the percentage of the total load to be connected to a telephone loop which is used by the device, to prevent overloading. The termination on a loop may consist of any combination of devices subject only to the requirement that the total of the Load Numbers of all the devices does not exceed 100.

Important safety instructions

Australian Safety Information

The following safety information is provided in conformance with Australian safety requirements:

CAUTION: DO NOT USE BEFORE READING THE INSTRUCTIONS: Do not connect the Ethernet, Phone 1 and Phone 2 ports to a carrier or carriage service provider's telecommunications network or facility unless: a) you have the written consent of the network or facility manager, or b) the connection is in accordance with a connection permit or connection rules.

Connection of the Ethernet, Phone 1, and Phone 2 ports may cause a hazard or damage to the telecommunication network or facility, or persons, with consequential liability for substantial compensation.

Caution

- The direct plug-in power supply serves as the main power disconnect; locate the direct plug-in power supply near the product for easy access.
- For use only with CSA Certified Class 2 power supply, rated 12VDC, 1.5A.

Telecommunication installation cautions

- Never install telephone wiring during a lightning storm.
- Never install telephone jacks in wet locations unless the jack is specifically designed for wet locations.
- Never touch uninsulated telephone wires or terminals unless the telephone line has been disconnected at the network interface.
- Use caution when installing or modifying telephone lines.
- Avoid using a telephone (other than a cordless type) during an electrical storm. There may be a remote risk of electric shock from lightning.
- Do not use the telephone to report a gas leak in the vicinity of the leak.

Battery

The Netopia R310's lithium battery is designed to last for the life of the product. The battery is not user-serviceable.

Caution!

Danger of explosion if battery is incorrectly replaced.

Replace only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions.

Glossary

Access Line: A telephone line reaching from the telephone company central office to a point usually on your premises. Beyond this point the wire is considered inside wiring. See also *Trunk Line*.

analog: In telecommunications, telephone transmission and/or switching that is not digital. An analog phone transmission is one that was originally intended to carry speech or voice, but may with appropriate modifications be used to carry data of other types.

ANSI (American National Standards Institute): Devises and proposes recommendations for international communications standards. See also *Comite Consultatif International Telegraphique et Telephonique (CCITT*).

backbone: A network topology consisting of a single length of cable with multiple network connection points.

Bandwidth: The range of frequencies, expressed in Kilobits per second, that can pass over a given data transmission channel within a network. The bandwidth determines the rate at which information can be sent through a channel - the greater the bandwidth, the more information that can be sent in a given amount of time.

BAP: Bandwidth Allocation Protocol. Manages the dynamic bandwidth allocation of implementations supporting the PPP multilink protocol. This is done by defining the Bandwidth Allocation Protocol (BAP), as well as its associated control protocol, the Bandwidth Allocation Control Protocol (BACP). BAP can be used to manage the number of links in a multilink bundle.

baud rate: The rate of the signaling speed of a transmission medium.

bit: A binary digit; the smallest unit of data in the binary counting system. A bit has a value of either 0 or 1.

bits per second (bps): A measure of the actual data transmission rate. The bps rate may be equal to or greater than the baud rate depending on the modulation technique used to encode bits into each baud interval. The correct term to use when describing modem data transfer speeds.

bps: See *bits per second*.

branch: A length of cable in a star network that goes from the center of the star to a wall jack.

broadcast: A network transaction that sends data to all hosts connected to the network.

Burstiness: Data that uses bandwidth only sporadically; that is, information that does not use the total bandwidth of a circuit 100 percent of the time. During pauses, channels are idle; and no traffic flows across them in either direction. Interactive and LAN-to-LAN data is bursty in nature, because it is sent intermittently, and in between data transmission the channel experiences idle time waiting for the DTEs to respond to the transmitted data user's input of waiting for the user to send more data.

byte: A group of bits, normally eight, which represent one data character.

CallerID: See *CND.*

CCITT (Comite Consultatif International Telegraphique et Telephonique): International Consultative Committee for Telegraphy and Telephony, a standards organization that devises and proposes recommendations for international communications. See also *ANSI (American National Standards Institute)*.

CHAP (challenge handshake protocol): A method for ensuring secure network access and communications.

Class A, B, and C networks: The values assigned to the first few bits in an IP network address determine which class designation the network has. In decimal notation, Class A network addresses range from 1.X.X.X to 126.X.X.X, Class B network addresses range from 128.1.X.X to 191.254.X.X, and Class C addresses range from 192.0.1.X to 223.255.254.X. For more information on IP network address classes, see Appendix D, "Understanding IP Addressing."

client: An intelligent workstation that makes requests to other computers known as servers. PC computers on a LAN can be clients.

clustering: A feature that clusters remapped network numbers into a range of sequential network numbers.

CNA (Calling Number Authentication): A security feature that will reject an incoming call if it does not match the Calling Number field in one of the Netopia ISDN Router's Connection Profiles.

CND (Calling Number Delivery): Also known as caller ID, a feature that allows the Called Customer Premises Equipment (CPE) to receive a calling party's directory number during the call establishment phase.

community strings: Sequences of characters that serve much like passwords for devices using SNMP. Different community strings may be used to allow an SNMP user to gather device information or change device configurations.

CRC (Cyclic Redundancy Check): A computational means to ensure the integrity of a block of data. The mathematical function is computed, before the data is transmitted at the originating device. Its numerical value is computed based on the content of the data. This value is compared with a recomputed value of the function at the destination device.

DCE (Data Communications Equipment): Term defined by standards committees, that applies to communications equipment, typically modems or printers, as distinct from other devices that attach to the network, typically personal computers or data terminals (DTE). The distinction generally refers to which pins in an RS-232-C connection transmit or receive data. Also see *DTE*.

DTE (Data Terminal Equipment): Term defined by standards committees, that applies to communications equipment, typically personal computers or data terminals, as distinct from other devices that attach to the network, typically modems or printers (DCE). The distinction generally refers to which pins in an RS-232-C connection transmit or receive data. Pins 2 and 3 are reversed. Also see *DCE*.

default zone: When a Phase II EtherTalk network includes more than one zone, all routers on that network must be configured to assign one of these zones as a default zone. The default zone is temporarily assigned to any Phase II EtherTalk node that hasn't chosen a zone. The user may choose another zone by opening the Network Control Panel, selecting the correct physical connection, and then choosing a zone in the scrolling field displayed.

DHCP (Dynamic Host Configuration Protocol): A service that lets clients on a LAN request configuration information, such as IP host addresses, from a server.

DNS (Domain Name Service): A TCP/IP protocol for discovering and maintaining network resource information distributed among different servers.

download: The process of transferring a file from a server to a client.

EIA (Electronic Industry Association): A North American standards association.

Ethernet: A networking protocol that defines a type of LAN characterized by a 10 Mbps (megabits per second) data rate. Ethernet is used in many mainframe, PC, and UNIX networks, as well as for EtherTalk.

Ethernet address: Sometimes referred to as a hardware address. A 48-bits long number assigned to every Ethernet hardware device. Ethernet addresses are usually expressed as 12-character hexadecimal numbers, where each hexadecimal character (0 through F) represents four binary bits. Do not confuse the Ethernet address of a device with its network address.

firmware: System software stored in a device's memory that controls the device. The Netopia ISDN Router's firmware can be updated.

gateway: A device that connects two or more networks that use different protocols. Gateways provide address translation services, but do not translate data. Gateways must be used in conjunction with special software packages that allow computers to use networking protocols not originally designed for them.

hard seeding: A router setting. In hard seeding, if a router that has just been reset detects a network number or zone name conflict between its configured information and the information provided by another router, it disables the router port for which there is a conflict. See also *non-seeding, seeding*, *seed router,* and *soft seeding*.

HDLC (High Level Data Link Control): A generic link-level communications protocol developed by the International Organization for Standardization (ISO). HDLC manages synchronous, code-transparent, serial information transfer over a link connection. See also *SDLC (Synchronous Data Link Control).*

header: In packets, a header is part of the envelope information that surrounds the actual data being transmitted. In e-mail, a header is usually the address and routing information found at the top of messages.

hop: A single traverse from one node to another on a LAN.

hop count: The number of nodes (routers or other devices) a packet has gone through. If there are six routers between source and destination nodes, the hop count for the packet will be six when it arrives at its destination node. The maximum allowable hop count is usually 15.

host: A single, addressable device on a network. Computers, networked printers, and routers are hosts.

Host Computer: A communications device that enables users to run applications programs to perform such functions as text editing, program execution, access to data bases, etc.

internet: A set of networks connected together by routers. This is a general term, not to be confused with the large, multi-organizational collection of IP networks known as the Internet. An internet is sometimes also known as an internetwork.

internet address, IP address: Any computing device that uses the Internet Protocol (IP) must be assigned an internet or IP address. This is a 32-bit number assigned by the system administrator, usually written in the form of 4 decimal fields separated by periods, e.g., 192.9.200.1. Part of the internet address is the IP network number (IP network address), and part is the host address (IP host address). All machines on a given IP network use the same IP network number, and each machine has a unique IP host address. The system administrator sets the subnet mask to specify how much of the address is network number and how much is host address. See also *Class A, B, and C networks*.

IP (Internet Protocol): A networking protocol developed for use on computer systems that use the UNIX operating system. Often used with Ethernet cabling systems. In this manual, IP is used as an umbrella term to cover all packets and networking operations that include the use of the Internet Protocol. See also *TCP/IP*.

IP address, IP host address, IP network address: See *internet address*.

IP broadcast: See *broadcast*.

IPX (Internet Package Exchange): A protocol used by Novell Netware networks.

ISDN (Integrated Services Digital Network): A method of transmitting data digitally over telephone lines.

ISP (Internet service provider): A company that provides Internet-related services. Most importantly, an ISP provides Internet access services and products to other companies and consumers.

ITU (International Telecommunication Union): United Nations specialized agency for telecommunications. Successor to CCITT.

K56flex: A modem data transmission technology standard created by Lucent Technologies and Rockwell International. Its purpose is to take advantage of the largely digital portions of the telephone system in order to exceed the theoretical speed limitations of data transmission over analog telephone lines. A competing technology called "x2," created by U.S. Robotics/3Com, performs a similar function. In February, 1998, the interested parties agreed on a unified standard called V.90, also known as V.PCM, which merges the K56flex standard with the competing x2 standard. In September, 1998, the International Telecommunications Union is expected to ratify the unified standard, thereby allowing interoperability of modems and ISPs' central site equipment, with appropriate firmware upgrades.

LAN (Local Area Network): A privately owned network that offers high-speed communications channels to connect information processing equipment in a limited geographic area.

MIB (Management Information Base): A standardized structure for SNMP management information.

modem: A device used to convert digital signals from a computer into analog signals that can be transmitted across standard analog (not ISDN) telephone lines. Modem is a contraction of modulator-demodulator.

NAT (Network Address Translation): A feature that allows communication between the LAN connected to the Netopia ISDN Router and the Internet using a single IP address, instead of having a separate IP address for each computer on the network.

NetBIOS: A network communications protocol used on PC LANs.

network: A group of computer systems and other computer devices that communicate with one another.

network administrator: A person who coordinates the design, installation, and management of a network. A network administrator is also responsible for troubleshooting and for adding new users to the network.

network log: A record of the names of devices, location of wire pairs, wall-jack numbers, and other information about the network.

network number: A unique number for each network in an internet.

network range: A unique set of contiguous numbers associated with an extended network; each number in a network range can be associated with up to 253 node addresses.

node: See *host*.

non-seeding: A router setting that causes it to request network number and zone information from any other routers on the network connected to the non-seeding port. If it receives this information, it begins to route packets through that port. See also *hard seeding, seeding*, *seed router,* and *soft seeding*.

packet: A group of fixed-length binary digits, including the data and call control signals, that are transmitted through an X.25 packet-switching network as a composite whole. The data, call control signals, and possible error control information are arranged in a predetermined format. Packets do not always travel the same pathway but are arranged in proper sequence at the destination side before forwarding the complete message to an addressee.

Packet-Switching Network: A telecommunications network based on packet-switching technology, wherein a transmission channel is occupied only for the duration of the transmission of the packet.

PAP (PPP authentication protocol): A method for ensuring secure network access.

Parameter: A numerical code that controls an aspect of terminal and/or network operation. Parameters control such aspects as page size, data transmission speed, and timing options.

port: A location for passing data in and out of a device, and, in some cases, for attaching other devices or cables.

port number: A number that identifies a TCP/IP-based service. Telnet, for example, is identified with TCP port 23.

POTS (Plain Old Telephone Service): Ordinary analog telephone service such as that used for voice transmission, as distinct from digital service.

PPP (Point to Point Protocol): A protocol for framing IP packets and transmitting them over a serial line.

protocol: A set of rules for communication, sometimes made up of several smaller sets of rules also called protocols. AppleTalk is a protocol that includes the LocalTalk, EtherTalk, and TokenTalk protocols.

remapping: See *network number remapping*.

RFC (Request for Comment): A series of documents used to exchange information and standards about the Internet.

RIP (Routing Information Protocol): A protocol used for the transmission of IP routing information.

RJ-11: A telephone-industry standard connector type, usually containing four pins.

RJ-45: A telephone-industry standard connector type usually containing eight pins.

router: A device that supports network communications. A router can connect identical network types, such as LocalTalk-to-LocalTalk, or dissimilar network types, such as LocalTalk-to-Ethernet. However—unless a gateway is available—a common protocol, such as TCP/IP, must be used over both networks. Routers may be equipped to provide WAN line support to the LAN devices they serve. They may also provide various management and monitoring functions as well as a variety of configuration capabilities.

router port: A physical or logical connection between a router and a network. Where a network only allows the use of one protocol, each physical connection corresponds to one logical router port. An example is the Netopia ISDN Router's LocalTalk port. Where a network allows the use of several protocols, each physical connection may correspond to several logical router ports—one for each protocol used. Each router port has its own network address.

routing table: A list of networks maintained by each router on an internet. Information in the routing table helps the router determine the next router to forward packets to.

seeding: A method for ensuring that two or more routers agree about which physical networks correspond to which network numbers and zone names. There are three options: non-seeding, soft seeding, and hard seeding. Seeding can often be set separately for each router port. See also *hard seeding*, *non-seeding, seed router,* and *soft seeding*.

seed router: A router that provides network number and zone information to any router that starts up on the same network. See also *hard seeding*, *non-seeding, seeding,* and *soft seeding*.

serial port: A connector on the back of the workstation through which data flows to and from a serial device.

server: A device or system that has been specifically configured to provide a service, usually to a group of clients.

SNMP (Simple Network Management Protocol): A protocol used for communication between management consoles and network devices. The Netopia ISDN Router can be managed through SNMP.

soft seeding: A router setting. In soft seeding, if a router that has just been reset detects a network number or zone name conflict between its configured information for a particular port and the information provided by another router connected to that port, it updates its configuration using the information provided by the other router. See also *hard seeding*, *non-seeding, seeding,* and *seed router*.

subnet: A network address created by using a subnet mask to specify that a number of bits in an internet address will be used as a subnet number rather than a host address.

subnet mask: A 32-bit number to specify which part of an internet address is the network number, and which part is the host address. When written in binary notation, each bit written as 1 corresponds to 1 bit of network address information. One subnet mask applies to all IP devices on an individual IP network.

SDLC (Synchronous Data Link Control): A link-level communications protocol used in an International Business Machines (IBM) Systems Network Architecture (SNA) network that manages synchronous, code-transparent, serial information transfer over a link connection. SDLC is a subset of the more generic HDLC (High-Level Data Link Control) protocol developed by the International Organization for Standardization (ISO).

TCP/IP (Transmission Control Protocol/Internet Protocol): An open network standard that defines how devices from different manufacturers communicate with each other over one or more interconnected networks. TCP/IP protocols are the foundation of the Internet, a worldwide network of networks connecting businesses, governments, researchers, and educators.

telephone wall cable: 2-pair, 4-pair, or 8-pair, 22- or 24-gauge solid copper wire cable. Telephone wall cable is sometimes called telephone station cable or twisted-pair cable.

TFTP (Trivial File Transfer Protocol/Internet Protocol): A protocol used to transfer files between IP nodes. TFTP is often used to transfer firmware and configuration information from a UNIX computer acting as a TFTP server to an IP networking device, such as the Netopia ISDN Router.

thicknet: Industry jargon for 10Base-5 coaxial cable, the original Ethernet cabling.

thinnet: Industry jargon for 10Base-2 coaxial cable, which is thinner (smaller in diameter) than the original Ethernet cabling.

UDP (User Datagram Protocol): A TCP/IP protocol describing how packets reach applications in destination nodes.

V.90: A modem data transmission standard, also known as V.PCM, which merges the K56flex standard with the competing x2 standard. In September, 1998, the International Telecommunications Union is expected to ratify the unified standard, thereby allowing interoperability of modems and ISPs' central site equipment, with appropriate firmware upgrades.

wall jack: A small hardware component used to tap into telephone wall cable. An RJ-11 wall jack usually has four pins; an RJ-45 wall jack usually has eight pins.

WAN (wide area network): A network that consists of nodes connected by long-distance transmission media, such as telephone lines. WANs can span a state, a country, or even the world.

WAN IP: In addition to being a router, the Netopia ISDN Router is also an IP address server. There are four protocols it can use to distribute IP addresses over the WAN which include: DHCP, BOOTP, IPCP and MacIP. WAN IP is a feature for Netopia ISDN Router models.

wiring closet: A central location where a building's telephone and network wiring is connected. Multi-story buildings often have a main wiring closet in the basement and satellite wiring closets on each floor.

Index

Limited Warranty and Limitation of Remedies

Netopia warrants to you, the end user, that the Netopia R310™ ISDN Router (the "Product") will be free from defects in materials and workmanship under normal use for a period of one (1) year from date of purchase. Netopia's entire liability and your sole remedy under this warranty during the warranty period is that Netopia shall, at its sole option, either repair or replace the Product.

In order to make a claim under this warranty you must comply with the following procedure:

1. Contact Netopia Customer Service within the warranty period to obtain a Return Materials Authorization ("RMA") number.
2. Return the defective Product and proof of purchase, shipping prepaid, to Netopia with the RMA number prominently displayed on the outside of the package.

If you are located outside of the United States or Canada, please contact your dealer in order to arrange for warranty service.

THE ABOVE WARRANTIES ARE MADE BY NETOPIA ALONE, AND THEY ARE THE ONLY WARRANTIES MADE BY ANYONE REGARDING THE ENCLOSED PRODUCT. NETOPIA AND ITS LICENSOR(S) MAKE NO OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, REGARDING THE ENCLOSED PRODUCT. EXCEPT AS OTHERWISE EXPRESSLY PROVIDED ABOVE, NETOPIA AND ITS LICENSOR(S) DO NOT WARRANT, GUARANTEE OR MAKE ANY REPRESENTATION REGARDING THE USE OR THE RESULTS OF THE USE OF THE PRODUCT IN TERMS OF ITS CORRECTNESS, ACCURACY, RELIABILITY, CURRENTNESS, OR OTHERWISE. THE ENTIRE RISK AS TO THE RESULTS AND PERFORMANCE OF THE PRODUCT IS ASSUMED BY YOU. THE EXCLUSION OF IMPLIED WARRANTIES IS NOT PERMITTED BY SOME STATES OR JURISDICTIONS, SO THE ABOVE EXCLUSION MAY NOT APPLY TO YOU. IN THAT CASE, ANY IMPLIED WARRANTIES ARE LIMITED IN DURATION TO NINETY (90) DAYS FROM THE DATE OF DELIVERY OF THE PRODUCT. THERE MAY BE OTHER RIGHTS THAT YOU MAY HAVE WHICH VARY FROM JURISDICTION TO JURISDICTION.

REGARDLESS OF WHETHER OR NOT ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL NETOPIA, ITS LICENSOR(S) AND THE DIRECTORS, OFFICERS, EMPLOYEES OR AGENTS OF ANY OF THEM BE LIABLE TO YOU FOR ANY CONSEQUENTIAL, INCIDENTAL OR INDIRECT DAMAGES (INCLUDING DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, AND THE LIKE) ARISING OUT THE USE OR INABILITY TO USE THE PRODUCT EVEN IF NETOPIA OR ITS LICENSOR(S) HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATIONS MAY NOT APPLY TO YOU. NETOPIA AND ITS LICENSOR(S) LIABILITY TO YOU FOR ACTUAL DAMAGES FROM ANY CAUSE WHATSOEVER, AND REGARDLESS OF THE FORM OF THE ACTION (WHETHER IN CONTRACT, TORT [INCLUDING NEGLIGENCE], PRODUCT LIABILITY OR OTHERWISE), WILL BE LIMITED TO $50. v.300